United States Department of Energy

National Training Center

Facility Security Officer Orientation Correspondence Course (*PHY-210DB)*

Student Workbook and Study Guide

August 2006 Version 1.1

U.S. DEPARTMENT OF ENERGY (DOE)
NATIONAL TRAINING CENTER (NTC)

The NTC is the Department of Energy's model training provider, recognized as a DOE "Training Center of Excellence." Through its various academies and training services, it is also a national training resource for the National Nuclear Security Administration; for other federal agencies; and for state, local, and international organizations involved in protecting national security assets. The NTC's parent organization is DOE's Office of Security and Safety Performance Assurance (SSA).

Mission

The NTC's primary mission is to promote the development, maintenance, and enhancement of a qualified and professional workforce with the competencies necessary to accomplish DOE missions through relevant and effective training and professional-development programs in technical disciplines, especially Safeguards, Security, and Safety.

History

In 1984 DOE created the Central Training Academy (CTA) in Albuquerque to train protective-force personnel in the skills necessary to protect U.S. nuclear facilities against terrorist threats. In the early 1990s the CTA expanded its mission to include all safeguards and security (S&S) topics and was redesignated the Safeguards and Security Central Training Academy (S&SCTA). Over the next two decades, the organization's mission evolved to address a wide range of new training needs, such that the curriculum eventually grew to include some 130 courses in all six S&S program elements: information security; nuclear materials control and accountability; personnel security; program and planning management (including curriculum development and instructional techniques); physical protection; and protective force.

In 1998 the organization became the Nonproliferation and National Security Institute and, in 2004, was renamed the National Training Center (NTC). The NTC's academies and training services now include—in addition to the original S&SCTA— the Counterintelligence Training Academy, the Foreign Interaction Training Academy, and the Safety Training Program, which develops and implements training for staff who have safety-related responsibilities at DOE defense nuclear facilities. Since the original organization's inception in 1984 and throughout its subsequent evolution, it has been operated by Wackenhut Services Incorporated.

Student-Centered Training Goals

Committed to *putting students first,* the NTC has established these training goals:

- Develop and deliver first-class, up-to-date training.
- Offer training in a variety of media, formats, and delivery methods.
- Apply state-of-the-art learning techniques that promote interactivity, student participation, networking opportunities, and personal as well as professional growth.
- Continuously evaluate, fine-tune, and upgrade training to meet students' changing needs.

This material was produced for and delivered to
the National Training Center by Wackenhut
Services Incorporated,
Palm Beach Gardens, Florida

UNITED STATES
DEPARTMENT OF ENERGY

NATIONAL TRAINING CENTER

FACILITY SECURITY OFFICER (FSO) ORIENTATION CORRESPONDENCE COURSE (PHY-210DB)

TABLE OF CONTENTS

UNITED STATES
DEPARTMENT OF ENERGY

NATIONAL TRAINING CENTER

FACILITY SECURITY OFFICER (FSO) ORIENTATION CORRESPONDENCE COURSE (PHY-210DB)

COURSE SYLLABUS

TITLE

Facility Security Officer Orientation Correspondence Course

LENGTH OF COURSE

Approximately 24 hours

MISSION AND PURPOSE

This self-paced correspondence course provides basic knowledge on the roles and responsibilities of the DOE or DOE-contractor facility security officer. The emphasis is on the knowledge associated with facility security officer roles and responsibilities, facility clearance requirements, personnel security, information security, incident reporting, and other related programs.

ATTENDEES

The course is designed for DOE and DOE-contractor safeguards and security personnel with current or future assigned facility security officer positions or functions.

PREREQUISITES

None

UNITED STATES
DEPARTMENT OF ENERGY

NATIONAL TRAINING CENTER

FACILITY SECURITY OFFICER (FSO) ORIENTATION CORRESPONDENCE COURSE (PHY-210DB)

COURSE COMPOSITION

Chapter		Hours
1.0	Facility Security Officer Roles and Responsibilities	1.0
2.0	Facility Clearance Requirements, FDAR and FOCI	4.0
3.0	Personnel Security	6.0
4.0	Information Security	6.0
5.0	Incident Reporting, Inquiry Process, and Infractions	4.0
6.0	Other Related Programs	3.0
		24.0

Time allocated to each chapter includes time to read the chapter and answer the review questions. It may not include sufficient time to read the referenced DOE directives.

UNITED STATES
DEPARTMENT OF ENERGY

NATIONAL TRAINING CENTER

FACILITY SECURITY OFFICER (FSO) ORIENTATION
CORRESPONDENCE COURSE (PHY-210DB)

GOALS AND OBJECTIVES

Overall Course Goal

The overall goal of this training is for the student, upon successful completion of this course, to better understand the roles and responsibilities associated with the facility security officer position.

CHAPTER TITLE: Facility Security Officer Roles and Responsibilities

Instructional Goal:

1.0 The goal of this chapter is to give newly assigned facility security officers (FSOs) a basic understanding of the facility security officer's (FSOs) roles and responsibilities.

Instructional Objectives:

At the conclusion of this chapter, the student will identify:

1.1 The primary *responsibility* of an FSO

1.2 The primary *role* of an FSO.

1.3 Factors that may influence the actual roles assigned to an FSO.

FACILITY SECURITY OFFICER (FSO) ORIENTATION CORRESPONDENCE COURSE (PHY-210DB)

GOALS AND OBJECTIVES (Cont.)

CHAPTER TITLE: Facility Clearance Requirements, FDAR, and FOCI

Instructional Goal:

2.0 The goal of this chapter is to give newly assigned facility security officers (FSOs) an awareness of the facility clearance process.

Instructional Objectives

At the conclusion of this chapter, the student will identify:

2.1 The document that formally registers a facility with the DOE.

2.2 The purpose served by the initial facility survey.

2.3 The purpose served by a facility self-assessment.

2.4 The facility importance rating associated with a given facility rating description.

2.5 The purpose of the Foreign Ownership, Control, or Influence (FOCI) program.

2.6 The purpose of the Contract Security Classification Specification Form (CSCS).

2.7 The job title of the security officer (for the facility under review) whose appointment is a requirement of the facility clearance program.

2.8 The relationship between the clearance level of *key management personnel* and a facility's clearance level.

FACILITY SECURITY OFFICER (FSO) ORIENTATION CORRESPONDENCE COURSE (PHY-210DB)

GOALS AND OBJECTIVES (Cont.)

CHAPTER TITLE: Personnel Security

Instructional Goal:

3.0 The goal of this chapter is to give newly assigned facility security officers (FSOs) an awareness of the DOE's personnel security activities, including the access authorization process, reporting requirements, reinvestigation, security awareness program, and human reliability programs.

Instructional Objectives:

At the conclusion of this chapter, the student will identify:

3.1 Documentation that must be included in a request for processing access authorizations.

3.2 The requirements for determination of access authorization level (Q or L).

3.3 The reinvestigation cycle for cleared individuals.

3.4 The mandatory reporting requirements for individual contractors holding active access authorizations.

3.5 The time constraints for meeting mandatory reporting requirements.

3.6 When each of the four mandatory Safeguards and Security Awareness Program briefings is to be provided to personnel.

FACILITY SECURITY OFFICER (FSO) ORIENTATION CORRESPONDENCE COURSE (PHY-210DB)

GOALS AND OBJECTIVES (Cont.)

3.7 The forms requiring completion:
DOE F 5631.18 – *Security Acknowledgement Form*
DOE F 5631.29 – *Security Termination Statement*
SF-86 – *Questionnaire for National Security Positions* (QNSP)
Form FD-258 – *Fingerprint Card*
DOE F 5631.34 – *Data Report on Spouse/Cohabitant*
SF-312 – *Classified Information Nondisclosure Agreement*
DOE F 472.1 – *Fair Credit Reporting Act Notification and Release*

3.8 The type of positions that fall under the Human Reliability Program (HRP)

3.9 The main purpose served by the HRP.

3.10 The factors evaluated by the HRP.

3.11 Additional requirements imposed on the individual by the HRP.

FACILITY SECURITY OFFICER (FSO) ORIENTATION CORRESPONDENCE COURSE (PHY-210DB)

GOALS AND OBJECTIVES (Cont.)

CHAPTER TITLE: Information Security

Instructional Goal:

4.0 Upon completion of this lesson, students will have an awareness of Classified Matter Protection and Control (CMPC), classification/declassification of information, unclassified/ classified Information System Security (ISS), and the Operations Security Program (OPSEC).

Instructional Objectives:

At the conclusion of this chapter, the student will identify:

4.1 How the classification is determined for information or material that needs to be protected in the interest of national security.

4.2 The three levels of classified information.

4.3 The three categories of classified information.

4.4 The minimum marking that each inside page of classified documents must possess.

4.5 The terms associated with sensitive unclassified information.

4.6 Descriptions of important Classified Matter Protection and Control (CMPC) requirements.

4.7 Characteristics of the declassification process.

FACILITY SECURITY OFFICER (FSO) ORIENTATION CORRESPONDENCE COURSE (PHY-210DB)

GOALS AND OBJECTIVES (Cont.)

4.8 The required security/protection plan *documents* that specify details of the DOE contractor's approach to ensuring protection of computer and communications resources.

4.9 Additional responsibilities assumed by personnel who use classified information in performance of duties, i.e., users.

4.10 The objectives of the OPSEC Program.

4.11 The means by which an individual could release sensitive information.

FACILITY SECURITY OFFICER (FSO) ORIENTATION CORRESPONDENCE COURSE (PHY-210DB)

GOALS AND OBJECTIVES (Cont.)

CHAPTER TITLE: **Incident Reporting, Inquiry Process, and Infractions**

Instructional Goal:

5.0 Upon completion of this chapter, students will have an awareness of the inquiry process associated with incidents of safeguards and security concern.

Instructional Objectives:

At the conclusion of this chapter, the student will identify:

5.1 The description of terms associated with the inquiry process.

5.2 Examples of infractions.

5.3 The time constraints imposed by DOE directives on responding to incidents of safeguards and security concern.

5.4 The agency to whom an incident is reported if an inquiry establishes that a violation occurred.

5.5 The agency to whom an incident is reported if an inquiry establishes credible information that fraud, waste, and/or abuse has occurred.

5.6 Examples of employee responsibilities in the inquiry process.

5.7 Characteristics of typical administrative contractor-disciplinary actions of infractions.

FACILITY SECURITY OFFICER (FSO) ORIENTATION CORRESPONDENCE COURSE (PHY-210DB)

GOALS AND OBJECTIVES (Cont.)

CHAPTER TITLE: **Other Related Programs**

Instructional Goal:

6.0 Upon completion of the chapter, students will have an awareness of physical security requirements, Materials Control and Accountability (MC&A), and requirements for reporting fraud, waste, and abuse.

Instructional Objectives:

At the conclusion of this chapter, the student will identify:

6.1 The types of DOE security areas..

6.2 Examples of prohibited articles.

6.3 Examples of controlled articles.

6.4 The two basic elements of the MC&A program.

6.5 Three materials designated as special nuclear material (SNM) by DOE

6.6 The meaning of the term “graded safeguards” for nuclear materials.

6.7 Two of the factors that determine the level of protection provided for SNM.

FACILITY SECURITY OFFICER (FSO) ORIENTATION CORRESPONDENCE COURSE (PHY-210DB)

EVALUATION

EVALUATION

Student performance will be evaluated by means of a written test (open book) for which the minimum passing score is 80% on each end-of-lesson test. Any student scoring below 80% on any test at the end of each chapter will receive remediation through the lead instructor.

An administrator's guide accompanies the student workbook and includes an answer key, an explanation of the correct answer for each test item, a scoring chart, and an objectives-to-examination question matrix. The final examination questions are the review questions found in the student workbook.

DOE NATIONAL TRAINING CENTER

Completion & Student Feedback Form: (Self-Study)

Name: _____ Job Title: _____

POC/Organization: _____ POC or Supervisor Signature: _____

Course Title: **Facility Security Officer (PHY-210DB)** Completion Date: _____ Grade: _____ %

Please help us improve our training and materials by answering the following questions. Your reactions, comments, and suggestions are needed and appreciated.

Please rate the following:

We encourage you to offer comments and suggestions concerning any ratings.

		Not Applicable	Poor	Fair	Good	Very Good	Excellent
1.	The clarity of the instructions for using this training was...	❑	1	2	3	4	5
2.	The organization of the training was...	❑	1	2	3	4	5
3.	The ease of navigation through the program was... (Computer-based and Web-based training only)	❑	1	2	3	4	5
4.	The usefulness of the review questions was...	❑	1	2	3	4	5
5.	The level of detail in the course material was...	❑	1	2	3	4	5
6.	The overall quality of the training was...	❑	1	2	3	4	5

7. What parts of the training were **most useful**?

_____

_____

_____

8. How could this training be improved? (Amount/quality of the information presented, types of graphics and illustrations used, acquiring the training from NTC, etc.)

_____

_____

_____

9. Identify the agency/functional area under which your job falls.

a. ❑ DOE ❑ NNSA ❑ OTHER AGENCY

b. ❑ M&O ❑ National Laboratory ❑ Sub-contractor (tier II or III)

c. ❑ Safeguards & Security
❑ Emergency Operations
❑ Counterintelligence
❑ Foreign Visits/Assignments
❑ Other_____

d. ❑ Scientist
❑ Principal Investigator
❑ Engineer
❑ Academician
❑ Laboratory Operations
❑ Laboratory Support Services

10. Why did you take this course? _____

11. How many years of work experience do you have in the training's subject area? _____

12. Are you taking the course to fulfill a PEP or ADAPT requirement? ❑ Yes ❑ No
If yes, please note which: _____

Additional comments:

FACILITY SECURITY OFFICER ORIENTATION CORRESPONDENCE COURSE (PHY-210DB)

Reference material cited or used in the Facility Security Officer Orientation Correspondence Course:

United States Department of Energy Orders and Manuals:

DOE O 470.4, *Safeguards and Security Program,* 8-26-05

DOE M 470.4-1, Chg. 1, *Safeguards and Security Program Planning and Management,* 3-7-06

DOE M 470.4-2, Chg. 1, *Physical Protection,* 3-7-06

DOE M 470.4-3, Chg. 1 *Protective Force,* 3-7-06

DOE M 470.4-4, *Information Security,* 8-26-05

DOE M 470.4-5, *Personnel Security,* 8-26-05

DOE M 470.4-6, *Nuclear Material Control and Accountability,* 8-26-05

DOE M 470.4-7, *Safeguards and Security Program References,* 8-26-05

DOE M 475.1-1A *Identifying Classified Information,* 2-26-01

DOE M 471.2-2 *Classified Information Systems Security,* 8-3-1999

DOE O 205.1 *Cyber Security Program,* 3-21-03

United States Atomic Energy Act of 1954 and Title 18 of the United States Code

United States Department of Energy
Design Basis Threat Guidance (U)

U.S. Code of Federal Regulations (CFR), Part 710, *General Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material*.

Sandia National Laboratories
Sandia Report SAND93-2030, *"Overview of Locking Systems," 1993*

United States Army Manual FM 19-30, Physical Security

United States Department of Energy
Security Container and Locking Device Guide, October 1993

THIS PAGE LEFT BLANK INTENTIONALLY

Chapter 1: Facility Security Officer Roles and Responsibilities

Goal

The goal of this chapter is to give newly assigned facility security officers (FSOs) a basic understanding of the FSO's roles and responsibilities.

Objectives

Upon successful completion of this chapter, you will be able to identify the following:

- The primary *responsibility* of an FSO.
- The primary *role* of an FSO.
- Factors that may influence the actual roles assigned to an FSO.

FSO Overview

As cited in DOE M 470.4-7, FACILITY SECURITY OFFICER (FSO). A U.S. citizen, with an access authorization equivalent to the facility clearance, assigned the responsibility of administering the requirements of the S&S Program within the facility. To meet the requirements of the National Industrial Security Program Operating Manual (NISPOM), the contractor Facility Security Officer (FSO) and key management personnel must possess access authorizations equivalent to the level of the facility clearance (for information on facility clearances see DOE M 470.4-1, Chg. 1, *Safeguards and Security Program Planning and Management*).

> Every organization performing safeguards and security tasks and services for the U.S. Department of Energy (DOE) is required* to appoint its own FSO. Examples of these organizations are DOE offices, prime contractors to DOE, or subcontractors to a prime contractor. The DOE, the prime contractor, and the subcontractors each appoint their own FSOs to serve as security points of contact (POCs). More important than being a POC, the FSO is responsible for administering the requirements of the Safeguards and Security Program within his or her facility, i.e., ensuring that proper levels of protection are provided to prevent unacceptable, adverse impact on national security or on the health and safety of DOE and contractor employees, the public, or the environment.

In addition to complying with the DOE requirements, companies operating under the auspices of the National Industrial Security Program may have additional training requirements. These requirements will be based on the company's or facility's involvement with classified information, and may include an FSO orientation course and for FSOs at facilities with safeguarding capability, an FSO Program Management Course.** Training if required, should be completed within one year of appointment to the FSO position.

* **DOE M 470.4-1 Chg 1**, Chapter VI - FACILITY CLEARANCE

***NISPOM Chapter 3, Paragraph 3-102*

Role of the FSO

This course provides basic knowledge of the roles and responsibilities of the DOE or DOE-contractor FSO. The importance of the FSO's role within the organization cannot be overstated. In serving as the company's point of contact (POC) for any security-related matter, he or she directs the implementation of security measures and is responsible for coordinating implementation of a security program with the prime contractor or DOE. The FSO is instrumental in making sure that personnel are aware of good security procedures and practice them, regardless of whether they have access to classified information or other DOE security interests. FSOs see that the organization's employees know their responsibilities regarding security procedures.

The duties assigned to FSOs can vary widely depending on the nature of the FSOs' organizations. For example, whether or not the FSO's office location is physically separated from the location where employees' work can have an impact on the FSO's role. Another factor is whether the company is a *possessing* facility (one that stores classified matter or special nuclear material at its own location).

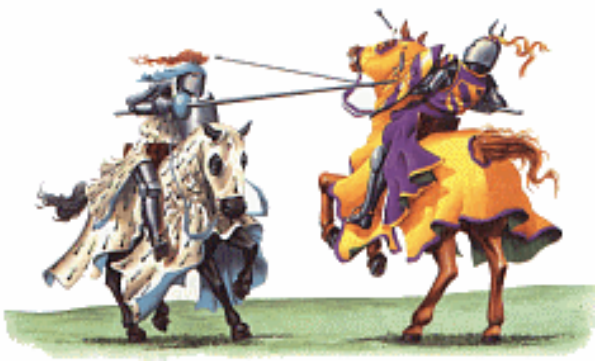
Another influencing factor is how many FSOs the organization has. If, for example, a DOE-contractor company has a main corporate headquarters as well as branch offices, the company may need more than one FSO. If so, the roles of the FSOs within the same company may differ. The corporate FSO may provide the necessary direction, share corporate security knowledge, and serve as a resource to FSOs in branch offices. Although the roles assigned to FSOs may vary, their primary responsibility remains constant: The FSO is responsible for administering the requirements of the Safeguards and Security Program within his or her facility, i.e., ensuring that proper levels of protection are provided to prevent unacceptable, adverse impact on national security or on the health and safety of DOE and contractor employees, the public, or the environment. Simply put, FSOs ensure that security policies and procedures are followed and this mission is accomplished. They accomplish this through teamwork with the subcontractor, prime contractor, and DOE. **DOE M 470.4-1, Chg. 1,** outlines the FSO appointment.

Review Questions for Chapter 1

1. The primary responsibility of an FSO is
   a. providing guidance to DOE and DOE prime contractor FSOs.
   b. administering the requirements of the DOE Safeguards and Security Program within their facilities.
   c. determining what responsibilities they want to assume and for which they will be held accountable.
   d. overridden by the responsibilities of the FSOs to their individual companies or organizations.

2. The primary role of an FSO is
   a. providing guidance to DOE and DOE-prime-contractor FSOs.
   b. serving as the company's point of contact (POC) for security-related matters.
   c. determining what responsibilities the DOE's FSOs are required to assume and for which they will be held accountable.

3. Which of the following are factors that may influence the actual roles assigned to a FSO?
   a. Whether the facility is "possessing" or "nonpossessing."
   b. Whether personnel are physically separated from the FSO's office.
   c. The organizational structure of the company.
   d. All the above.



Chapter 2: Facility Clearance Requirements, FDAR, and FOCI

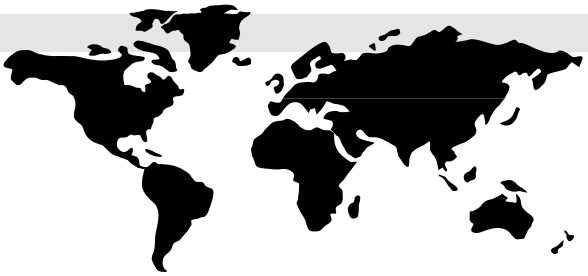
Goal

The goal of this chapter is to give newly assigned facility security officers (FSOs) an awareness of the facility clearance process.

Objectives

Upon successful completion of this chapter, you will be able to identify the following:

1. The facility importance rating associated with a given facility rating description.
2. The purpose of the Foreign Ownership, Control, or Influence (FOCI) program.
3. The purpose of the Contract Security Classification Specification Form (CSCS).
4. The relationship between the clearance level of certain company *key management personnel* and a facility's clearance level.
5. The job title of the facility security officer (for the facility under review) whose appointment is a requirement of the facility clearance program.
6. The purpose served by the initial facility survey.
7. The purpose served by a facility self-assessment.
8. The document that formally registers a facility with the DOE.



Overview

The *facility clearance program* regulates Departmental approval of a facility's eligibility to access, receive, generate, reproduce, store, transmit, or destroy classified matter, Special Nuclear Material, other hazardous material presenting a potential radiological or toxicological sabotage threat, and/or over $5,000,000 of DOE property exclusive of facilities and land value (collectively, safeguards and security (S&S) activities). Using a required set of factors, the facility clearance program evaluates a facility to determine its ability to meet Departmental S&S protection standards. Because the terminology used by DOE in the facility clearance program actually simplifies its explanation, please refer to the **DOE M 470.4-7, Safeguards and Security Program References** for a clarification of the "DOE meaning" of key words and phrases used in this course.

Facility Clearance Program

DOE requires that a *facility clearance* be granted to a facility before any performance of safeguards and security activities is permitted. The terms *facility*, *facility clearance*, and *safeguards and security activities* have DOE-specific meanings — meanings exclusive to a DOE environment.

FACILITY. An educational institution, manufacturing plant, laboratory, office building, or complex of buildings located on the same site that is operated and protected by the Department, the U.S. Nuclear Regulatory Commission, or their contractors.

FACILITY CLEARANCE. An administrative determination that a facility is eligible to access, receive, produce, use, and/or store classified matter, nuclear materials, or Departmental property of significant monetary value.

SAFEGUARDS AND SECURITY ACTIVITY. Any work performed under contract, subcontract, or other agreement which involves access to classified information, nuclear material, or Departmental property of significant monetary value by the Department, a Departmental contractor, or any other activity under the Department's jurisdiction. Also included is the verification of the capabilities of approved Federal locations.

It is important to note that the term *facility clearance*, as used in this chapter, applies to both the *contractor clearance* (for nonpossessing facilities) and the *contractor facility clearance* (for possessing facilities).

Accepting a Contractor's Existing Federal Agency Facility Clearance

A contractor holding facility clearance from another federal agency may be approved by DOE for processing, using, or storing classified matter, contingent on certain conditions (see **DOE M 470.4-1 Chg 1**). This

reciprocity between DOE and the other Government agency must be documented in a written agreement prior to the acceptance of the facility clearance.

For a facility clearance to be considered valid and acceptable for use on a fully reciprocal basis by another federal department or agency, it must meet or exceed the level of clearance needed. However, the other federal agency's facility clearance will not be accepted if it is based on a Special Security Agreement, Security Control Agreement, or Limited Facility Clearance.

Requirements

Using a required set of factors as a "yardstick," the DOE *facility clearance program* evaluates a facility to determine its ability to meet Department S&S protection standards. Approval of a facility is based on favorable results and approvals on all required factors. The key required factors (explained in detail on later pages) are the following:

- Submission of Facility Data and Approval Record (FDAR), [DOE F 470.2]. This may not be required if the subcontractor is listed on the prime contractor's FDAR.
- Completion of an initial facility survey with Satisfactory facility rating determination (excepting non-possessing facilities, which are not required to have a facility survey).
- Determination of Foreign Ownership, Control, or Influence (FOCI)
- Development of Site Safeguards and Security Plan (SSSP), or Site Security Plan (SSP)
- Completion of Contract Security Classification Specification (CSCS), [DOE F 470.1].
- Appointment of a Facility Security Officer (FSO)
- Obtainment of access authorizations for appropriate personnel (e.g., those key management personnel who must be cleared with and to the level of the facility clearance).

Subcontractors usually submit required documentation to the prime contractor's organization. Prime contractors submit the required documentation directly to DOE. Ultimately, the documentation will go to the appropriate DOE lead responsible office (LRO). A discussion of these required factors follows (for an expanded discussion of *access authorizations,* see **DOE M 470.4-5, Personnel Security**).

SSIMS

The Safeguards and Security Information Management System (SSIMS) is a classified database used as a master repository of safeguards and security information and issues on government and contractor facilities with security interests. SSIMS is used to record information including facility approvals, facility administrative information, and documentation on facility surveys/inspections (i.e., ratings, findings, corrective actions, etc.).

Requirement*: FDAR*

The facility data and approval record (FDAR) is the form that formally registers a facility with DOE. Some think of the FDAR as the facility's "birth certificate." It is the documentation necessary for the organization to be considered approved to use, store, process, or perform work relative to DOE S&S interests.

The FDAR (DOE F 470.2) is typically completed by the organization's procurement or business operations office (*initiator*). The DOE lead responsible office (LRO) is responsible for recording the FDAR into the SSIMS.

The SSIMS entry will identify the highest importance level of S&S activity for the facility under review. The initiator's organization will be notified of its assigned importance rating as a normal part of the facility clearance process.

Requirement : Facility Survey or Self-Assessment

An initial S&S survey of the facility must be conducted before the facility (except for non-possessing facilities) is considered for certification by the facility clearance process.

Surveys are assessments of the protection afforded S&S interests within a facility. They include examination of the devices, equipment, personnel, and procedures employed at the facility to protect classified or sensitive matter, special nuclear material, and/or DOE property *to ensure compliance and performance* with DOE requirements.

The *Initial Facility Survey* (one of four types of surveys) is required for possessing facilities. A comprehensive initial survey is *not* required as part of the facility clearance program for nonpossessing facilities because they do not possess safeguards and security interests at their site, but will be assessing safeguards and security interests only at another cleared facility (ies) at which a comprehensive initial facility survey was conducted. Only the *initial facility survey* is discussed in this course, because it is an integral part of the facility clearance program. Other types of surveys (in addition to the initial survey) may also be conducted as part of the facility clearance program, depending on the type of facility.

DOE G 470.1-2, **SAFEGUARDS AND SECURITY SURVEY AND SELF-ASSESSMENT GUIDE** identifies the initial survey as "a comprehensive survey conducted at the facility before granting approval" of the facility. A satisfactory initial survey establishes the eligibility of the facility and results in the completion of the Facility Data Approval Record (FDAR). To ensure the establishment and implementation of appropriate protective measures,

special emphasis should be placed on documentation and on the performance testing of staff to ensure procedures have been implemented and understood."

DOE M 470.4-1 Chg 1, **Safeguards and Security Program Planning and Management** contains specific information about the survey process. For your information, a series of training courses (both correspondence and resident) covering the DOE survey processes is available from NTC. See the NTC Website (http://www.ntc.doe.gov/ntc/) for an online course catalog.

In contrast to a survey, a *self-assessment* is an *internal* (the organization looking at itself) monitoring of the facility's S&S programs and activities to ensure compliance with S&S requirements. The self-assessment process employs internal inspections, reviews, or audits, or some combination of the three. Self-assessments are to be conducted at approximately the midpoint between the periodic surveys conducted by the Department's surveying office. For facilities that do not have classified matter, special nuclear material, or property protection interests (i.e., non-possessing facilities), self-assessments are part of the self-assessments for the sites or facilities at which the non-possessing facilities reside.

(Refer to DOE M 470.4-1 Chg 1 *for more detailed information.)*

Although there are differences between surveys and self-assessments, there are also similarities: Both facility *surveys* and *self-assessments* must cover all applicable topical and subtopical elements identified on the DOE form, *Safeguards and Security Survey/Inspection Report* (**DOE F 470.8**).

The survey form **DOE F 470.8** can be found on the DOE Forms WebPages. (http://www.directives.doe.gov/forms/index.html*)*

As the FSO for your facility, your familiarity with "The Big Picture" of the facility clearance program will facilitate participation in the process.

Facility Rating

Facility importance ratings provide a means of identifying the type of S&S facility and/or the type of S&S activities offered by a company seeking to do business with the Department. The FDAR and the initial facility survey are used as the basis for assigning an importance rating to the facility. Remember, a non-possessing facility is exempt from the initial survey requirements.

DOE has established the facility importance rating system as a means of identifying protection goals and setting priorities. Depending on the mission of the facility and the materials found there, it is assigned an importance rating, e.g., Class A, B, C, D, E, PP, or NP.

The highest level of protective effort focuses on Class A facilities; Class PP facilities are lower in priority but should also be protected at a level consistent with their property value. The seven facility-importance ratings, described more fully in the Safeguards and Security Survey and Self-Assessment Guide (DOE G 470.1-2 Section 2), are as follows:

Rating "A"

This rating is assigned to activities and facilities that are

- Engaged in administrative activities essential to the direction and continuity of the overall DOE nuclear weapons program, according to determination by heads of Headquarters elements or field officers.
- Authorized to possess Top Secret matter.
- Authorized to possess Category I quantities of special nuclear material (SNM).

Rating "B"

This rating is assigned to activities and facilities that meet any of the following criteria:

- Engaged in activities other than those categorized as "A" and authorized to possess Secret Restricted Data and/or weapons data.
- Designated as a Field Intelligence Element (FIE).
- Authorized to possess Category II quantities of SNM.

Rating "C"

This rating is assigned to activities and facilities that meet any of the following criteria:

- Authorized to possess Categories III and IV quantities of SNM or other nuclear materials requiring safeguard controls or special accounting practices.
- Authorized to possess classified matter other than the type categorized for "A" and "B" facilities.

Rating "D"

This rating is assigned to activities and facilities that provide common carrier, commercial carrier, or mail service. These facilities are not authorized to

store classified matter or nuclear material. Carriers who *do* must be assigned an "A," "B," or "C" importance rating.

Rating "E" (Excluded Parent)

This rating is assigned to a corporate tier "parent" of a contractor organization that has been barred from participation in the activities related to a contract with DOE.

Rating "PP" (Property Protection)

This importance rating is assigned to facilities to which a special standard of protection must be applied. These special standards are applied when a facility has

- Government property of a significant monetary value ($5 million or more).
- Nuclear materials other than those categorized as types "A," "B," "C," that require safeguard controls or special accounting procedures.
- DOE program continuity.
- National security considerations.
- Responsibilities for protection of public health and safety.
- Basic considerations that include physical protection to prevent or deter acts of arson, civil disorder, riots, sabotage, terrorism, vandalism, and theft or destruction of DOE property and facilities.

Rating "NP" (Nonpossessing)

This rating is assigned to facilities that have authorized access to classified information or special nuclear materials at other approved locations. Nonpossessing facilities do not, themselves, possess any classified matter or nuclear material.

Requirement: FOCI

A Foreign Ownership, Control, or Influence (FOCI) determination is required for contractors that will have employees and key management personnel with access authorizations. The FOCI program reviews ownership of the company seeking facility clearance approval and the extent of any foreign involvement. The FOCI program is designed to protect the common defense and security against undue risk, if access authorization makes classified information or

special nuclear materials available to contractors or subcontractors whose companies are owned, controlled, or influenced by foreign interests. Facility clearance will not be granted until all relevant aspects of FOCI have been resolved and, if necessary, are favorably adjudicated. Additionally, an existing facility clearance will be suspended, or may be terminated, for a contractor determined to be under FOCI.

The contractor receives from the DOE LRO a *Guidance Package* for completing the FOCI submission. The FOCI program requires the contractor to fill out a questionnaire (SF 328, Certificate Pertaining to Foreign Interests) certifying the accuracy of the answers, that defines the extent and nature of any FOCI over the contractor. The answers are verified by the DOE LRO before he or she renders a favorable FOCI determination. If any of the thresholds for FOCI determination are exceeded, the FOCI package is forwarded to DOE-HQ, who in turn will make a FOCI determination. If DOE believes there is a substantial risk due to the contractor's FOCI, the Department halts the facility clearance process until the contractor takes DOE-approved action to isolate the unacceptable FOCI.

Refer to **DOE M 470.4-1 Chg 1** for more FOCI requirements. NTC's training courses — *Introduction to FOCI* (PPM-150) and *FOCI* (PPM-151) — can provide additional information. See the NTC Website (http://www.ntc.doe.gov/ntc/) for an online course catalog.

FOCI Reporting Requirements

The FSO should be aware of the FOCI reporting requirements placed on his or her company by DOE M 470.4-1 Chg 1 and paragraph 1-302 of the National Industrial Security Program Operating Manual, which requires contractors to accomplish the following task:

1. Report any material changes concerning previously reported FOCI information.

2. Submit an updated SF 328 every five years even if the company reports no change.

These reporting requirements apply to all DOE-registered facilities.

The Contract Security Classification Specification Form (CSCS) DOE F 470.1

The Contract Security Classification Specification Form (CSCS, DOE F 470.1) is used to register contracts, subcontracts, and contractor solicitations that require DOE access authorizations. This data is maintained as part of SSIMS. The CSCS is the basic means for documenting classification, regrading, and declassification specifications or information pertaining to supplies, service, and other matters to be furnished by the contractor to the

government (or by the government to the contractor). The FSO is responsible for making certain this is done.

Requirement: **Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP)**

The SSSP or SSP documents the facility's potential threat, potential targets within the site, and the site's protection strategies, including the details of site physical protection measures required by DOE M 470.4-1 Chg 1.

An SSSP is required only if the facility will possess classified matter or special nuclear material. Sometimes additional security plans will be needed to address protection programs for specialized types of operations. At a facility where an SSSP is *not* required (because of the limited scope of safeguards and security interests), a site security plan (SSP) is required to describe the protection programs in place.

For more information about the SSSP (in addition to that found in DOE M 470.4-1 Chg 1), the following resources are suggested:

- DOE SSSP Guide: Acceptance Criteria Review Guide and Security Plans, April 1996.
- DOE Site Safeguards and Security Plan Acceptance Criteria and Review Guide (no date).
- Several NTC courses touch on this subject, e.g., *Vulnerability Assessment Fundamentals* (CTA-140) and various survey courses. See the NTC Website — http://www.ntc.doe.gov/ntc/— for an online course catalog.

Requirement: **Appointment of a Facility Security Officer (FSO)**

Appointment of a U.S. citizen to be the FSO is required as a part of facility clearances. Name and phone number must be noted on the FDAR.

As covered in the next section, the FSO must possess a personnel clearance (access authorization) equivalent to the facility clearance.

Responsibilities of the FSO include:

1. Serving as the point of contact with the DOE LRO/other applicable Department Elements and having the responsibility for oversight and implementation of all security-related activities at the facility; and
2. Communicating to the DOE LRO any new safeguards and security activities or changes in safeguards and security activities via numerous vehicles including, but not limited to: new or revised security plans,

DOE F 470.1 CSCS's; implementation plans for new security requirements or modified Departmental Directives; corrective action plans.

Requirement: ***Access Authorizations for Appropriate Contractor Personnel***

As required by DOE M 470.4-1 Chg 1 and the National Industrial Security Program Operating Manual (NISPOM), access authorizations for certain officials are mandatory prior to the issuance of a facility clearance requiring a classified level of clearance. This requirement normally involves the owners, officers, directors, partners, trustees, or executive personnel (i.e., key management personnel (KMP)). This requirement also includes the FSO and any employee designated to succeed the FSO, during permanent or temporary absence. These KMP must be cleared with and to the level of the facility clearance. Failure of these KMP to obtain and to continue to hold the appropriate level clearance will make the company ineligible for a facility clearance and any existing facility clearance would be administratively terminated. Based on their need for access, all other KMP must be cleared at the facility level, cleared at a lower level, or excluded from being cleared. If cleared at a lower level or not cleared, the company's board of directors or similar governing body must take formal exclusion action.

Refer to DOE M 470.4-1 Chg 1 and paragraphs 2-104 and 2-106 of the NISPOM. See Chapter 3 of this course for further discussion of *access authorizations*.

Note: For more information FOCI or the FOCI process, the FSO should enroll in the NTC S&SCTA course PPM-151: Foreign Ownership, Control, or Influence course.

Review Questions for Chapter 2

1. Each site or facility performing safeguards and security activities for DOE is required to be registered and approved by DOE. Which of the following documents serves to formally *register* a facility with DOE?

   a. Form 470.8 Safeguards and Security Survey/Inspection Report

   b. Form 470.1 Contract Security Classification Specification

   c. Form 470.2 Facility Data and Approval Record (FDAR)

   d. Safeguards and Security Information Management Systems (SSIMS) Report

   e. FOCI Survey Data Sheet

2. Within the DOE's facility clearance approval program, the purpose served by the *Initial Facility Survey* is to

   a. ensure the establishment and implementation of appropriate protective measures within a facility.

   b. determine where classified matter is stored.

   c. serve as a master protection strategy document for the facility.

   d. assess the extent and nature of any foreign ownership, control, or influence over the contractor.

3. As opposed to the purpose of a survey, the purpose served by a *self-assessment* is to

   a. independently determine where special nuclear materials are stored.

   b. develop a site security strategy document.

   c. internally monitor the facility's S&S programs and activities to ensure compliance with S&S requirements.

   d. serve as a site security strategy document for the facility.

4. Which of the DOE facility importance ratings does the following information describe?
   "This rating is assigned to facilities that have access authorizations to classified information or special nuclear material at other approved locations. Nonpossessing facilities do not, themselves, possess any classified matter."

   a. Rating "A"

   b. Rating "B"

   c. Rating "PP"

   d. Rating "NP"

5. The purpose of the DOE Foreign Ownership, Control, or Influence (FOCI) program is to determine

   a. the facility importance rating.

   b. whether foreign involvement with a DOE contractor poses an undue risk to the common defense and security in accordance with established FOCI policy.

   c. which facilities should be surveyed.

   d. what information should be classified.

6. The Contract Security Classification Specification Form (CSCS) is used to

   a. document requests for access authorizations.

   b. register requests to classify facilities.

   c. register any requests for proposal.

   d. register contracts, subcontracts, and solicitations that require access authorization.

7. What is the *job title* of the security officer whose appointment is a requirement of the facility clearance program for the facility under review?

   a. Facility officer

   b. Security facility contact

   c. Facility security officer

8. Certain key management personnel of the company seeking facility clearance approval must

   a. be cleared with and to the level of the facility clearance.

   b. not be cleared unless they are working at the site.

   c. not be cleared at the level of the facility clearance unless the FSO deems it necessary.

Chapter 3: DOE Personnel Security

Goal

The goal of this chapter is to give newly assigned facility security officers (FSOs) an awareness of the most salient DOE personnel security activities including the access authorization process, reporting requirements, and security awareness.

Objectives

Upon successful completion of this chapter, you will be able to:

1. State the purpose of the DOE Personnel Security Program
2. Identify sources of guidance for the DOE Personnel Security Program
3. Differentiate between the two types of DOE access authorizations and their respective levels of access
4. Identify the investigative requirements associated with the two types of DOE access authorizations.
5. Recognize two adjunct programs associated with the DOE Personnel Security Program
6. Identify general requirements and actions associated with processing initial DOE access authorization requests
7. List individual reporting requirements and associated time constraints for persons applying for or holding a DOE access authorization
8. List contractor (i.e., company) reporting requirements and associated time constraints of conditions affecting an applicant's or employee's access authorization status
9. State the purpose of the DOE Safeguards and Security Awareness Program
10. Detail the four mandatory Safeguards and Security Awareness briefings

The DOE Personnel Security Program

Purpose

The DOE Personnel Security Program is the cornerstone of a comprehensive safeguards and security system. The purpose of the DOE Personnel Security Program is to ensure that individuals with access to classified information and special nuclear materials (SNM) do not pose a threat to the nation's security. Indeed, it is the policy of DOE to "…allow access…only when it has been determined that such access will not endanger the common defense and security and is clearly consistent with the national interest" (DOE O 470.4-5).

Sources of Guidance

DOE access authorization rules/regulations are specified in Title 10 of the U.S. Code of Federal Regulations (CFR), Part 710, *General Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material*. Part 710 is commonly referenced as "10 CFR 710" and consists of one subpart. Subpart A concerns general criteria and procedures common to the overall DOE Personnel Security Program.

Detailed implementing requirements, responsibilities, and procedures associated with the DOE Personnel Security Program are provided in a DOE order and manual.

DOE Manual 470.4-5, *Personnel Security,* 8-26-05, provides detailed requirements and procedures for the DOE Personnel Security Program.

In addition to the above documentation, also consider the NTC's *Introduction to DOE Personnel Security* Self-Study Course (PER-100DB) for supplemental understanding of select DOE personnel security activities.

Access Authorization

DOE Access Authorization Types

An access authorization is an administrative determination that an individual is eligible for access to classified matter or SNM on a need-to-know basis. As a general rule, only U. S. citizens are eligible for access authorizations. DOE access authorization types are designated Q or L. The type of access authorization requested depends on the category (RD, FRD, or NSI) and level (Top Secret, Secret, or Confidential) of classified matter and/or category of SNM (I, II, III, or IV) to which the individual requires access on a need-to-know basis. The general relationship between Q and L and the permitted categories/levels of access to classified matter or SNM is provided in the figure below.

		Classified Matter Categories		
		RD	FRD	NSI
Classification Levels	TS	Q	Q	Q
	S	Q	Q&L	Q&L
	C	Q&L	Q&L	Q&L

SNM Category	Access Auth.
I	Q
II With Credible Roll-Up To I	Q
II & III	L
IV	None

Access Authorization Matrices

Investigative Requirements

The FBI has historically completed background investigations for a limited number of senior DOE officials and, since early 2001, conducts investigations for all positions defined as "high risk," such as the Human Reliability Program (HRP) and/or access to Sensitive Compartmented Information (SCI). For the vast majority of remaining cases, the Office of Personnel Management (OPM) performs the investigation. Both the FBI and OPM commonly contract out this function.

The investigative agency gathers facts and issues a report of its findings that vary in scope and depth depending on the type of access authorization required. Unless an adequate investigative report is already available, the local personnel security staff must normally obtain

- A Single Scope Background Investigation (SSBI) for every Q access authorization applicant
- An Access National Agency Check and Inquiry (ANACI) for an L access authorization for federal applicants
- A National Agency Check with Local Agency Checks and Credit Check (NACLC) for an L access authorization for contractor applicants

In addition to these applicant investigations, a reinvestigation program is in place to ensure that individuals with an access authorization is periodically reevaluated to determine their continued need for such access authorization and reinvestigated to determine their continued eligibility.

The type of reinvestigation to be conducted is determined by the type of access authorization held by the individual and the recertification by the individual's sponsor of the individual's continued need for access.

For holders of a Q access authorization, reinvestigation takes place at each 5-year interval following completion of the previous investigation or reinvestigation. For holders of an L access authorization, reinvestigation takes place at each 10-year interval following completion of the previous investigation or reinvestigation. Notice of the reinvestigation, including instructions and submission deadlines will be made directly to the individual and may include notice to the FSO as well.

Upon receipt of the investigative report from the FBI or OPM, DOE alone makes the access authorization determination and is sole authority responsible for adjudicating the case and taking any other adjudicative actions.

Adjunct Programs

DOE has established two adjunct programs as methods to effectively accommodate unique circumstances within the field of personnel security: the Human Reliability Program (HRP) and the Accelerated Access Authorization Program (AAAP).

The HRP is detailed in 10 CFR 712. In addition to an access authorization, it requires screening and periodic evaluation of individuals who apply for or occupy certain positions that are especially critical to the national security. The HRP involves four components: supervisory review, medical assessment, management evaluation, and security determination. To be placed in the H, a position must afford direct access to Category I quantities of SNM, have direct responsibility for transporting or protecting Category I quantities of SNM, afford unescorted access to the control areas of nuclear material production reactors, or have the potential for causing unacceptable damage to the national security.

AAAP is a program that provides the means for the Director, Office of Security, to grant an interim access authorization prior to completion of the standard personnel security process. The program does not replace the normal background investigation process, but is designed to accommodate a limited number of justifiable requests for an expedited Q access authorization for DOE mission critical work. Participation in the program is completely voluntary and involves a psychological evaluation, drug testing, and a counterintelligence polygraph examination. Contact your cognizant DOE personnel security office for additional details.

General Requirements for Access Authorizations

Initial Requests

An applicant's employer normally initiates the personnel security process by submitting a request for an access authorization to the cognizant DOE personnel security office. Each request must include

- The type of access authorization required for the position.

- Detailed justification, including the specific duties requiring access and the categories and levels of classified information or category of SNM to be accessed. Note that operational convenience is *not* justification for requesting an access authorization (e.g., to establish a pool of cleared employees in anticipation of unspecified classified work; to preclude the use of access controls or physical barriers to distinguish perimeters between security areas and open areas; to alleviate responsibilities for escorting uncleared individuals within a security area; or to determine an individual's suitability for employment).

The sponsor should request the specific type of access authorization required to avoid unnecessary expenditure of DOE funds and resources as well as the unwarranted invasion of an individual's privacy.

Requests for access authorizations should not be submitted until the sponsor has been awarded a DOE contract and has submitted the required paperwork for a Foreign Ownership, Control, or Influence (FOCI) determination. Although a clearance request may be submitted to DOE pending completion of a FOCI determination, a favorable FOCI determination is a necessary prerequisite for an access authorization to be granted.

Required Forms

Required security forms and instructions for requesting access authorizations are provided by the cognizant DOE office. Typically, the sponsor submits the request to DOE, who reviews it and, if it is approved, initiates further processing actions. The necessary forms depend on whether the applicant is a federal or contractor employee. Federal applicants must submit the following:

- Standard Form 86 (SF- 86), Questionnaire for National Security Positions. The SF-86 is the standard U.S. Government form used as the basis for a security clearance investigation.

- SF- 87, Fingerprint Card. Personnel obtaining prints must be adequately trained to recognize unclassifiable prints. Retakes delay the access authorization process.

- Either SF-171, Application for Federal Employment; Optional Form 612 (OF-612), Optional Application for Federal Employment; or a resume. These forms are applicable only to applicants for federal employment.

- DOE F 5631.18, Security Acknowledgement. This form contains information on DOE clearance criteria, select reporting requirements,

and other responsibilities imposed upon an individual being considered for a DOE access authorization.

- DOE F 472.1, Release (Fair Credit Reporting Act of 1970, as amended). This form serves as notification of rights under the Act and as the release from the clearance applicant/holder for DOE to obtain credit information.

Contractor applicants must submit the same forms except those associated with application for federal employment. A different fingerprint card, Form FD-258, is also required. In addition, contractor requests must include

- The DOE contract or subcontract number
- Certification of the individual's U.S. citizenship
- Preemployment checks required by 48 CFR 970.2201(b)(1)(ii) for employees of management and operating (M&O) contractors or other contractors managing DOE-owned sites/facilities.

In the event the applicant currently has a security clearance/access authorization granted by another federal agency or has had one in the past, a DOE access authorization may be granted under certain circumstances through reciprocity or reinstatement, respectively.

Several types of classified information require, in addition to an access authorization, programmatic approval before access to the information is authorized. These include

- Sensitive Compartmented Information (SCI)
- Weapon data
- North Atlantic Treaty Organization (NATO) information
- Cryptographic (CRYPTO) or Communications Security (COMSEC) information

Notification of Determination

The final determination regarding an individual's initial eligibility is provided in writing or electronically to the company security representative (e.g., FSO). DOE does not provide this notification directly to the individual, unless that individual is also the designated company official who usually receives them or if the request for access authorization is denied. In the case of reinvestigation, the individual may be given notification of access authorization continuation upon request.

Administrative Review

The DOE administrative review (AR) process establishes procedures for the examination of questions concerning an individual's eligibility for a DOE access authorization when it is determined that such questions cannot be favorably resolved by other actions. The objective is to ensure that denials or revocations of access authorization are fair and provide due process. In the case of AR, the individual in question is contacted directly. DOE AR procedures are set forth in 10 CFR 710 §§ 710.20 through 710.32.

Individual Reporting Requirements

Individuals applying for or granted DOE access authorizations must

- Provide full, frank, and truthful answers to relevant and material questions, and when requested, furnishing or authorizing others to furnish information that DOE deems pertinent to the access authorization eligibility process. This applies when completing security forms, during the course of an initial investigation and reinvestigations, and at any stage of access authorization processing including but not limited to letters of interrogatory, personnel security interviews, DOE-sponsored mental evaluations, and other authorized DOE investigative activities. An individual may elect not to cooperate; however, such refusal may prevent DOE from granting or continuing access authorization. In this event, any access authorization then in effect may be terminated or further processing may be suspended.

- Provide direct notification, verbally within 2 working days followed by written notification within the next 3 working days, to the cognizant DOE office of the following

    1. All arrests, criminal charges (including charges that are dismissed), or detentions by Federal, State, or other law enforcement authorities for violations of the law, other than traffic violations for which only a fine of $250 or less was imposed, within or outside of the United States;

    2. Personal or business-related filing for bankruptcy;

    3. Garnishment of wages;

    4. Legal action effected for name change;

    5. Change in citizenship;

    6. Employment by, representation of, or other business-related association with a foreign or foreign-owned interest, or foreign national; and

7. Hospitalization or other treatment for a mental illness; treatment for drug abuse; or treatment for alcohol abuse.

- Provide notification to the cognizant DOE office or the FSO, as appropriate, immediately after any approach or contact by any individual seeking unauthorized access to classified matter or SNM. If such an approach or contact is made while on foreign travel, individuals should notify a Department of State official at the local United States Embassy or Consulate with a request that the Department of State report the incident to the Director, Office of Security, at DOE Headquarters. This requirement is in addition to any similar reporting requirements implemented under DOE Orders or regulations

- Provide a completed DOE F 5631.34, "Data Report on Spouse/ Cohabitant," directly to the cognizant DOE office within 45 calendar days of marriage to, or cohabitation with, an individual who does not currently hold access authorization. This form states that "…a cohabitant is defined as an individual with whom you live, other than a legal spouse, child, or other relative (in-laws, mother, father, brother, sister, etc.), with whom you have a spouse-like relationship or similar bond of affection."

Note that the requirements for the individual to report circumstances of security interest directly to the cognizant DOE office do not preclude the contractor (i.e., company) from requiring the individual to also report these circumstances to the contractor's personnel security office or FSO.

Contractor (i.e., company) Reporting Requirements

Except for item 3 below, verbal notification within 2 working days followed by written confirmation within the next 10 working days shall be provided through established channels to the cognizant DOE office of the following conditions affecting an applicant's or employee's access authorization status:

1. When an applicant declines the offer of employment or fails to report for duty

2. When any of the following occur

   - Employment by the contractor is terminated;

   - Access authorization is no longer required;

   - The individual is on a leave of absence or on extended leave and will not require access for 90 consecutive calendar days. Upon request, this interval may be adjusted at the discretion of the cognizant DOE office;

- Access to classified matter or SNM is no longer required due to transfer to a position not requiring such access [NOTE: The cognizant DOE office may approve a contractor request for an individual to retain an access authorization when the contractor verifies that the individual shall be reemployed or reassigned by the contractor within the next 3 months in a position that will require an access authorization. The contractor must inform the cognizant DOE office of the individual's employment status at the end of the 3-month interval.]; or

- The individual leaves for foreign travel, employment, assignment, education, or residence of more than 3 months duration not involving official United States Government business. [NOTE: This requirement applies even if the individual remains employed by the contractor.]

3. When aware of an individual's hospitalization or other treatment for a mental illness or other condition that may cause a significant defect in the individual's judgment or reliability;

4. When made aware of information of personnel security interest. Such information must be characterized as reliable and relevant and create a question as to an individual's access authorization eligibility as exemplified in 10 CFR 710.8 (see the reverse of DOE F 5631.18);

5. When a foreign national under the contractor's cognizance becomes a United States citizen through naturalization or effects any other change in his/her citizenship status; or

6. When the contractor restricts or withdraws an employee's access to classified matter or SNM without DOE direction.

Safeguards and Security Awareness

The Safeguards and Security Awareness Program is an important component of the DOE Personnel Security Program. Safeguards and Security awareness is designed to ensure that both cleared and uncleared individuals are continually aware of their safeguards and security responsibilities. Greater detail on the DOE Safeguards and Security Awareness Program may be found in DOE M 470.4-1, Chg. 1, *Safeguards and Security Program Planning and Management,* Section K.

Every DOE site or facility having Security Areas, classified matter, and/or SNM is required to develop, implement, and maintain a Safeguards and Security Awareness Program.

Briefings

Briefings make up the heart of any security awareness program. Each program must include the development and presentation of at least four briefings:

- Initial
- Comprehensive
- Refresher
- Termination

All employees must receive an *initial* S&S awareness briefing, while only cleared individuals are required to receive the *comprehensive*, *annual*, and *termination* briefings.

The extent to which the FSO will be responsible for mandatory briefings differs from organization to organization. It is influenced by the organization's Site Safeguards and Security Plan/Site Security Plan agreement with the lead responsible office or the prime contractor's FSO.

Initial Briefing

The initial briefing is given to all individuals, cleared and uncleared, who are newly hired, or newly assigned to a facility or transferred to a new site, to acquaint them with the facility's programs, activities, and security procedures and their own security responsibilities.

The initial briefing must be completed before individuals report to their work areas, generally as a part of in-processing. When employment or assignment coincides with access authorization, initial and comprehensive security briefings may be combined.

The initial briefing may be presented through various methods that include oral presentations, videotapes, and computer- and Web-based briefings. They may be supported by employee handouts, such as:

- A Security handbook
- List of reporting requirements
- List of controlled and prohibited articles
- Site map
- Samples of document cover sheets and markings
- List of security contacts
- Current security newsletter

Required briefing subjects are described in DOE M 470.4-1, Chg. 1. Subjects include

- Facility overview
- Classification and access authorization procedures
- Protection of unclassified controlled information
- Badging and access control procedures
- Prohibited articles
- Property protection procedures
- Reporting responsibilities
- Substance abuse policies

Comprehensive Briefing

The comprehensive briefing is given to individuals granted DOE access authorizations and to cleared individuals who are being transferred between organizational elements to a new primary working environment. The purpose of the briefing is to inform individuals of the laws, policies and procedures regulating classified matter and of their security responsibilities for the protection and control of classified matter. As a condition of access to classified matter, individuals must complete the Standard Form 312, *Classified Information Nondisclosure Agreement* (SF-312).

After an access authorization is granted, the individual must be given a comprehensive security briefing before he or she is given access to classified matter or SNM. This briefing should be conducted as soon as possible after the access authorization is granted. When this process coincides with the beginning of employment, initial and comprehensive briefings may be combined.

Comprehensive briefings are presented through various methods to include oral presentations, videotapes, and computer- and Web-based briefings, supported by employee handouts. Examples of handouts are:

- List of reporting requirements for access authorization holders
- Samples of document cover sheets (e.g., Secret, Confidential) and markings
- Examples of incidents requiring notification to local security office
- Classified information matrices

When possible, this briefing should involve subject matter experts from other security-related programs. It should be coordinated with the job-specific briefing that cleared individuals will receive on classified matter protection and control (CMPC) to avoid duplication.

Security Awareness Coordinators often include information in the comprehensive briefing that satisfies the requirements of other security-related programs. Required briefing subjects are described in DOE M 470.4-1, Chg. 1, and are detailed in several DOE orders and manuals.

Refresher Briefing

A refresher briefing is required annually for all individuals who have access authorization. The objectives are to supplement, update, and reinforce security-related knowledge; to sustain heightened awareness of security issues; and to motivate fulfillment of security responsibilities.
A refresher briefing is presented annually at approximately a 12-month interval.

Security offices maintain a record of individuals who possess access authorizations. If the briefing is presented in a group setting, the Security Awareness Coordinator must coordinate attendance at refresher briefings with Security or with administrative representatives of the site/facility organizations. These representatives will notify individuals of the requirement to attend specific briefings and announce administrative sanctions for failure to attend. One or more make-up briefings may be required to achieve full compliance.

The refresher briefing offers a critical opportunity to influence and affect a person's understanding and knowledge of security. It is essential that coordinators stay aware of local and national security developments, issues, and concerns. The need to develop effective presentations on specific and sometimes sensitive issues makes networking and information exchange among coordinators highly desirable.

The refresher briefing is delivered by various methods, including oral presentation, videotapes, and computer- and Web-based presentations. Guest speakers, games, puzzles, and promotional items such as pens or memo pads can also serve as effective means of reinforcement for briefing points or general security awareness.

The briefing must selectively reinforce the information provided in the comprehensive briefing. Security developments over time, site-specific considerations, recent security incidents, and current events can guide subject selection. Suggestions for briefing content are:

- Reporting requirements
- CMPC requirements and procedures
- UCNI
- OUO
- Need-to-know criteria
- Escorting procedures

- Insider threat
- Hostile intelligence threat

Every effort should be made to make these briefings informative and interesting.

Termination Briefing

A termination briefing is required whenever an individual's access authorization has been or will be terminated. The termination briefing is given to impress upon each individual the continuing responsibility not to disclose classified information to which the person had access and the obligation to return all wholly or partially classified documents and materials in the person's possession to the appropriate DOE official. The briefing must also cover the potential penalties for noncompliance.

The termination briefing must be conducted on the individual's last day of employment, the last day the individual possesses an access authorization, or the day it becomes known that the individual no longer requires access to classified matter or SNM, whichever is sooner.

A site's Human Resources office typically notifies the site Security Office when an individual with an access authorization is to be terminated. A contractor or subcontractor company also notifies site Security of a cleared employee's termination. When it is determined that an individual no longer requires an access authorization, notification must be made electronically or verbally to the cognizant DOE Personnel Security organization within two working days.

The termination briefing may be provided by personnel outside of the Security Awareness Program. Security Awareness Coordinators should ensure that persons delivering the briefing are aware of the responsibilities for content and documentation.

The termination briefing may be delivered by various methods, including oral presentation, videotapes, and computer- and Web-based presentations. Under unique circumstances, a termination briefing can be accomplished by mail, phone, fax, or with the assistance of a representative of another organization or facility.

The obligations accepted in signing the SF-312 remain in effect even after an access authorization is terminated, and items 3, 4, 5, 7, and 8 of that document must be emphasized. Furthermore, completion of a termination security briefing requires that individuals give their assurance that all classified matter in their possession or charged to them has been returned to designated parties or destroyed in accordance with security directives. This assurance is given by signing DOE F 5631.29, "Security Termination Statement," in which an

individual repeats his/her pledge not to reveal any classified information except as authorized in writing by DOE officials empowered to give such permission. See Figure 2 for a copy of the DOE F 5631.29.

The briefing must include the penalties for unauthorized disclosure of classified information and UCNI as specified in the Atomic Energy Act of 1954 and Title 18 of the United States Code.

The Security Termination Statement, DOE F 5631.29, must be completed and forwarded to the cognizant DOE office that maintains the site/facility's Personnel Security files.

To document the briefing in the local Security Office, a copy of the signed DOE F 5631.29 may be filed or an alternate briefing verification form may be used as documentation if an individual is not available for this briefing, the unavailability must be documented on DOE F 5631.29 on the employee signature line, along with reason for termination.

Review Questions for Chapter 3

1. The DOE Personnel Security Program is the cornerstone of a comprehensive safeguards and security system.

    a. True
    b. False

2. Sources of guidance for the DOE Personnel Security Program include

    a. DOE O 472.1C
    b. DOE M 470.4-5
    c. 10 CFR 710
    d. All of the above
    e. None of the above

3. The type of access authorization requested for an individual depends on

    a. The category of classified matter and/or SNM to which to individual requires access
    b. The level of classified matter and/or SNM to which to individual requires access
    c. Need-to-know
    d. All of the above
    e. None of the above

4. The background investigation(s) normally required for an L access authorization include

    a. ANACI
    b. SSBI
    c. NACLC
    d. a & b
    e. a & c

5. The DOE AAAP Program

    a. Provides a means for expedited interim L access authorizations for mission critical work
    b. Involves a psychological evaluation, drug testing, and a counterintelligence polygraph
    c. Accommodates all requests for Q access authorizations
    d. Replaces the normal background investigation process
    e. Is not an adjunct program within the DOE Personnel Security Program

6. Justification for an access authorization should include

    a. The levels of classified information or category of SNM to be accessed
    b. The specific duties requiring access
    c. Items of operational convenience
    d. a & b
    e. b & c

7. Required forms for DOE access authorization requests common to <u>both</u> federal employees and contractors include

    a. The SF-86, SF-171, DOE F 5631.18, Fingerprint Card, and DOE F 472.1
    b. DOE F 472.1, DOE F 5631.18, SF 86, and Fingerprint Card
    c. Only the SF-86 and DOE F 5631.18
    d. Only the SF-86
    e. DOE F 5631.18 and DOE F 472.1

8. DOE Individual Reporting Requirements are applicable to

    a. Both applicants and holders of DOE access authorization
    b. Only applicants for DOE access authorization
    c. Only holders of DOE access authorization
    d. Only holders of DOE access authorization under reinvestigation
    e. None of the above

9. To whom are Individual Reporting Requirements reported?

    a. The FSO only
    b. The company security office only
    c. The cognizant DOE office
    d. The local law enforcement authority
    e. None of the above

10. How soon and in what manner must an individual report an arrest, criminal charge or detention by law enforcement authorities for violations of the law other than traffic violations for which only a fine ≤ $250 was imposed?

    a. Verbal notification only within 2 working days
    b. Verbal notification within 2 working days followed by written notification within the next 3 working days
    c. Written notification within 2 working days followed by verbal notification within the next 3 working days
    d. Written notification only within 3 working days
    e. Verbal notification within 3 working days followed by written notification within the next 2 working days

11. How soon and in what manner must a contractor (i.e., company) inform DOE of most of their reporting requirements?

    a. Verbal notification only within 10 working days
    b. Verbal notification within 2 working days followed by written confirmation within the next 3 working days
    c. Written confirmation within 10 working days followed by verbal notification within the next 2 working days
    d. Written confirmation only within 2 working days
    e. Verbal notification within 2 working days followed by written confirmation within the next 10 working days

12. The mandatory Safeguards and Security Awareness briefings consist of

    a. Job Specific, Comprehensive, Refresher, and Termination
    b. Termination, Comprehensive, and Refresher
    c. Refresher, Comprehensive, Initial, and Termination
    d. Refresher, Initial, Termination and Job Specific
    e. Initial, Comprehensive, and Termination

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 4: Information Security

Goal

Upon completion of this lesson, students will have an awareness of Classified Matter Protection and Control (CMPC), classification/declassification of information, unclassified/ classified Information System Security (ISS), and the Operations Security Program (OPSEC).

Objectives

Upon completion of this chapter, students will identify the following:

1. How the classification is determined for information or material that needs to be protected in the interest of national security.
2. The three levels of classified information.
3. The three categories of classified information.
4. The minimum marking that each inside page of classified documents must possess.
5. The terms associated with unclassified sensitive information.
6. Descriptions of important Classified Matter Protection and Control (CMPC) requirements.
7. Characteristics of the declassification process.
8. The required security/protection plan *documents* that specify details of the DOE contractor's approach to ensuring protection of computer and communications resources.
9. Additional responsibilities assumed by personnel who use classified information in performance of duties, i.e., users.
10. The objectives of the OPSEC Program.
11. The means by which an individual could release sensitive information.

Classification Authority

Classification is the process of identifying information that requires protection in the interests of preserving national security. In the United States there are currently two principal means by which classification system regulations are set forth: through Executive Orders (EOs) or through statutes.

- Executive Orders (EOs) are official documents, numbered consecutively, through which the President of the United States manages the operations of the federal government. An EO applies only to the federal government.

Statute Establishes "Restricted Data" (RD)

- A *statute* is legislation passed by Congress, and has greater applicability than an Executive Order (EO). A statute is the law of the land and applies to all citizens.

From 1946 to the present, our classification system [its three categories of classified are *Restricted Data* (RD), *Formerly Restricted Data* (FRD), and *National Security Information* (NSI)] has been founded on and regulated through both legislation and Executive Orders.

During the days when the Manhattan Project and the nation's nuclear research and development program were new, the very nature of atomic weaponry dictated that information concerning this devastating power be rigidly controlled. Domestic legislation to formalize control of sensitive information about nuclear weapons as well as control of the nation's nuclear weapons and research and development efforts was proposed and, when passed by Congress, became the Atomic Energy Act (AEA) of 1946.

The provisions of the AEA were enacted as legislation rather than an EO, because Congress and the President felt that information about nuclear weapons needed the strict regulation and enforcement afforded by statute. The AEA also established a new and separate category of classified information called *Restricted Data* (RD) that specifically targeted atomic energy information. RD was defined in section 10 of the Act as:

"...all data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power, but shall not include any data which the Commission from time to time determines may be published without adversely affecting the common defense and security."

Statute Establishes "Formerly Restricted Data" (FRD)

In the revised Atomic Energy Act of 1954, Congress established another new category of classified information, *Formerly Restricted Data* (FRD), for information concerning the military utilization of nuclear weapons. This was necessary because the Atomic Energy Act of 1946 transferred control of all aspects of atomic energy from military control to the civilian Atomic Energy Commission (AEC) and, as a stockpile of weapons was produced, the military was eager to have these weapons transferred to its control. The 1954 amendment allowed for some transfer of RD to the military by utilizing the new FRD classification category, defined in the 1954 amendment as

> "Classified information which has been removed from the Restricted Data category after DOE and DoD have jointly determined that it relates primarily to the military utilization of atomic weapons, and can be adequately safeguarded in the same manner as National Security Information."

Modifications to the AEA since 1954 include the addition of a section on Unclassified Controlled Nuclear Information (UCNI) in 1981.

Executive Orders Establish "National Security Information" (NSI)

Executive Orders form the basis of the *National Security Information* (NSI) classification system. NSI is defined as

> "...information which pertains to the national defense and foreign relations (National Security) of the United States and is classified in accordance with an Executive Order."

EOs and the National Industrial Security Program (NISP)

Various EOs lay out the rules governing the identification and protection of information, the unauthorized disclosure of which could cause "damage to the national security." Industrial contractors performing classified contracts are governed by the National Industrial Security Program (NISP), created in 1993 by Executive Order 12829, to "serve as a single, integrated, cohesive, industrial, security program to protect classified information." A supplement to the NISP, an operating manual (NISPOM), was issued in February 1995. It establishes standards for contractors involved with special access programs. The NISPOM is available from various sources, including http://nsi.org/Library/Govt/Nispom.html.

Classification Authority

Classification is the process of identifying information that should be protected in the interest of national security. By classifying information, an organization denies it to potential enemies while allowing scientists, engineers, and other cleared personnel with a need-to-know to use it. The fact that information is unclassified does not mean that it may be released to the public.

If information is determined to be classified under one of the three categories (RD, FRD, or NSI), it is assigned a classification level based on its potential to damage national security if disclosed to unauthorized persons. The three levels of classification, in descending order of potential damage, are **Top Secret (TS), Secret (S**), and **Confidential (C).**

- **Top Secret** is the classification level applied to information whose disclosure could reasonably be expected to cause exceptionally grave damage to the national security.
- **Secret** is the classification level applied to information whose unauthorized disclosure could reasonably be expected to cause serious damage the national security.
- **Confidential** is the classification level applied to information whose unauthorized disclosure could reasonably be expected to cause damage to the national security or cause undue risk to the common defense and security.

The three categories of classified information discussed earlier in this chapter, in descending order of importance and sensitivity, are as follows: **Restricted Data (RD), Formerly Restricted Data (FRD),** and **National Security Information (NSI)**. To summarize:

- **Restricted Data** is information that relates to the design, manufacture, or utilization of nuclear weapons, the production of special nuclear material (SNM), or the use of SNM in the production of energy. It is "born classified."
- **Formerly Restricted Data** is information that relates primarily to the military use or storage of nuclear weapons and that the DOE and the Department of Defense (DoD) have jointly decided to remove from the RD category.
- **National Security Information** is all information that protects the national security but does not relate to nuclear weapons or nuclear energy. NSI is classified when someone who is authorized decides that it should be classified.

NSI information is created in areas such as safeguards and security programs, nonproliferation and international security programs, and DOD-sponsored programs. Unlike RD, NSI is *not* "born classified."

A classifier is an individual who is authorized to determine whether information is – or is not – classified. A classifier is specially trained to make a classification determination in a particular area and apply a security classification to information or material. A classifier may have original classification authority or may derivatively assign a security classification.

A *derivative classifier* (also referred to as an authorized derivative classifier or ADC) is an individual authorized to determine whether documents or material are unclassified – or – classified based upon guidance derived from external sources (i.e., classification guide).

An *original classifier* is an individual authorized to classify National Security Information (NSI) by an original determination according to certain federal regulations. See DOE M 475.1-1A *Identifying Classified Information* 2-26-01, for more information on identifying classified information.

Proper Marking of Classified Documents

The mandatory marking requirements for classified documents vary according to classification level and category. At a minimum, classified matter must be marked with the classification level and classification category that have been assigned to it. See DOE M 475.1-1A for more detailed information.

Interior Pages: In a classified document, the classification *level* and *category* (if RD or FRD) are placed on both the top and bottom of each interior page and the back of the last page. For NSI, the classification *level* only is placed on the top and bottom of each interior page and the back of the last page. These markings must be distinguishable from the rest of the text.

Portion Marking: Classified documents containing *only* NSI require portion marking. This means each paragraph and subparagraph must be marked to reflect its classification. This marking must precede the paragraph or subparagraph. An authorized classifier can review the document and provide the necessary guidance for portion marking.

Other markings: If the information is RD or FRD, the classification *level* and *category* are placed on both the top and bottom of the outside of the front cover (if any) as well as the top and bottom of the back of the last page. If the information is NSI, only the classification *level* is placed on the front and back pages in this manner.

Title Marking: The title of the document must be annotated to indicate its classification level and category; the title marking must be present, even if it's "Unclassified."

Classifier Markings: The classifier applies the required classification markings, which include the following elements: the name or personal identifier of the classification authority (i.e., "Classified By"); position or title of the classifier; designation and date of source document(s) (if RD or FRD), or classification category (if NSI); duration of classification (NSI only); and office of origin.

SECRET

Originator's Identification _____
(Full Mailing Address)

Date

DEPARTMENT OF ENERGY
NATIONAL TRAINING CENTER

Title or Subject _____

FRONT COVER PAGE FOR SAMPLE DOCUMENT

CLASSIFIED FOR TRAINING USE ONLY

RESTRICTED DATA
This Document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions.

Classified by: (Name and Title)

Derived from: (Guide, Source, and Date)

SECRET

Unclassified Information (UCI)

Unclassified Information (UCI) refers to information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or governmental interests.

Types of UCI

The following are examples of UCI:

Unclassified Controlled Nuclear Information (UCNI) is sensitive government information that is controlled even though it is not classified because, if released, it could help a terrorist or saboteur gain access to nuclear materials or facilities. Orders for security police officers, engineering drawings, locations of special nuclear material storage units are examples of UCNI.

Export Controlled Information (ECI) is technical information that cannot be exported unless licensed by the Department of State, Department of Commerce, or Nuclear Regulatory Commission. Examples of ECI are specific details of design, production, or use of technology that has military or national security applications.

Official Use Only (OUO) applies to certain unclassified but sensitive administrative information.

Naval Nuclear Propulsion Information (NNPI) is information about the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, or repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated nuclear support facilities.

Company Proprietary applies to some sensitive documents that are from private companies or corporations.

Marking UCI

Certain types of UCI are to be marked appropriately. Several examples are noted.

Front Marking for UCNI consists of marking the front of the matter as follows:

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION
NOT FOR PUBLIC DISSEMINATION
Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168).

Reviewing Official: _____
(Name/Organization)

Date: _____

Guidance Used _____

Page Marking for UCNI consists of marking "UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION" or "UCNI" on the top and bottom of the front page and on the top and bottom of all interior pages of the matter – or at least on those interior pages that contain UCNI.

UCNI Special Formats (e.g., photographs, viewgraphs, films, magnetic tapes, floppy diskettes, audio or videotapes, slides) are marked so that both a person in physical possession of the matter and a person with access to the information in or on the matter are made aware that it contains UCNI.

OUO Marking involves marking "For Official Use Only" on the bottom of the front page and on the bottom of all interior pages of the matter – or at least on those interior pages that contain OUO.

With one exception, unclassified information is *not* normally marked "Unclassified." The exception occurs when marking is necessary to distinguish unclassified from classified information when unclassified occurs within classified material – and then only when such distinction serves a useful purpose to avoid confusion or to indicate that the information has been reviewed and found to be unclassified. See DOE O 471.1A *Identification and Protection of Unclassified Controlled Nuclear Information,* 6-30-2000, DOE M 475.1-1A, DOE O 470.4, *Safeguards and Security Program*, 8-26-05, and DOE M 470.4-4, *Information Security,* 8-26-05, for more information on document marking.

Protection and Control of Classified Matter

Ensuring that classified matter is not lost or compromised requires that classified information, regardless of its form, be afforded a level of protection against loss or compromise that is commensurate with its level of classification. It also requires personnel to protect classified matter from unauthorized and deliberate access. Various DOE directives provide detailed requirements for the protection and control of classified matter. These include DOE M 470.4-4 and DOE O 470.4.

The protection requirements described in these directives are consistent with the requirements set forth in the National Industrial Security Program (NISP) of 1993 and its supplemental Operating Manual (NISPOM) of 1995.

The goal of the Classified Matter Protection and Control (CMPC) program is to establish a system of procedures, facilities, and equipment to protect and control classified matter that is being generated, received, transmitted, used, stored, reproduced, or destroyed. Some important Classified Matter Protection and Control (CMPC) requirements are noted below.

Access

- Base access on a need-to-know.
- Require proper clearance for access.
- Use
- Protect documents from unauthorized access including visual access.
- Use designated Standard Form (SF) cover sheets on classified documents (SF 703 is the TOP SECRET cover sheet, SF 704 is the SECRET cover sheet, and SF 705 is the CONFIDENTIAL cover sheet).
- Ensure that classified matter is constantly attended by and/or under the control of authorized users.
- Custodians and authorized users of classified matter are responsible for the protection and control of such matter.
- Ensure that use, processing, or handling of classified matter is conducted only in security areas providing control measures at least equal to those present in limited areas.

Storage

- Store classified matter in an approved storage repository (safe, vault, vault-type room).
- The outside of the security container must NOT be marked to indicate the classification level of contents.
- Funds, firearms, medical items, controlled substances, precious metals, or other items susceptible to theft must NOT be stored in the same security container that is used to store classified matter.
- Store classified matter in a secured area that conforms to the applicable requirements of DOE O 470.4 and DOE M 470.4-4.

Transmission

- Only authorized individuals may remove documents from security areas.
- Documents to be transmitted outside a facility must be properly wrapped and secured.
- Documents must be transferred only through approved mail channels.
- Documents must be addressed only to approved classified addresses.
- Documents must be sent by approved mail messenger or hand-carried.
- Transmit documents only on fax machines approved for classified transmission.
- The FSO of the DOE LRO is to be notified whenever classified matter is to be hand-carried outside of the facility, to ensure that appropriate protection measures are implemented.

Reproduction

- Use only designated and approved copiers.
- Make only the minimum number of copies required.
- Legal and security postings for using a copier for classified documents must be posted near the classified copier.
- Reproduced copies are subject to the same protection and control requirements as the original.

Training

"Personnel whose responsibilities include the generation, handling/use, storage, reproduction, transmission, and/or destruction of classified matter must receive appropriate training to ensure such matter is not lost or compromised"(See DOE M 470.4-4) Contact the DOE LRO or the prime contractor's FSO for information regarding training programs that may be available.

FSOs may wish to take NTC's *Classified Matter Protection and Control* (CMPC) Self-Study Course (ISC-121DB) to further enhance their understanding of handling classified and sensitive matter (see http://www.ntc.doe.gov).

Declassification

Reducing the amount of information in the classification system allows for better management and cost controls of that system and increases respect for the information that needs to stay protected. Solving the problem of the growing backlog of classified documents requires the acceptance of *declassification* as a routine government activity. Declassifying means finding sensible, cost-effective, and routine ways to separate the categories of materials no longer warranting protection from those needing to stay secret.

All NSI (National Security Information) that has a *Specific Date or Event for Declassification* marking, (if it contains only NSI) is automatically declassified after the specified date or event has passed.

- Exemption from Automatic Declassification
  RD/FRD (Restricted Data/Formerly Restricted Data) is never *automatically* declassified, even if such documents or material also contain NSI. Such documents or material remain classified until an authorized person takes positive action to declassify them.

- NSI (National Security Information) *may* be exempt from automatic declassification under certain conditions, such as the following:

  1. *Without* a specific *Date for Declassification* marking, NSI is never automatically declassified.

  2. With an *Exemption from Declassification within 10 Years* marking, NSI is never *automatically* declassified.

  3. Historical Records that are 25 year old, contain only NSI, and are determined to be *Permanent Records* under Title 44 of the United States Code are never automatically declassified.

  4. Historical Records that are 25 year old, contain only NSI, and are determined to be *Temporary and Unscheduled Records* are never automatically declassified.

The "life-cycle approach" to classifying and protecting information incorporates a risk management philosophy (rather than one of nearly absolute risk avoidance) to decide how great is the risk and what countermeasures to apply. The life-cycle approach recognizes that both classified and unclassified information have a life span and that each type of record has its own distinct life cycle: records are born, reproduced, processed, consulted, reviewed, sent to the sidelines, brought back for consultation, possibly reborn into another document, and eventually end up in the trash or in permanent storage. Consideration of "how great is the risk and what countermeasures to apply" may lead to different results at different stages of the life cycle.

Classification of information means that resources will be spent throughout the information's life cycle to protect, distribute, and limit access to information. These expenses would be unnecessary if the information were not classified. Classifiers typically consider the *benefits* of classification without giving equal weight to its costs, an unbalanced approach that has led to *too much* classification and weakened protection of the nation's core secrets. By increasing the quality of classification reviews, we could reduce excessive initial classification. This would result in decreased physical protection costs for information that really does not warrant such protection.

DOE Openness Program and 10 CFR Part 1045—*Nuclear Classification and Declassification*

The Department of Energy is committed to a program that involves a comprehensive concerted effort to declassify and release information to the public, consistent with the requirements of national security. This policy is meant to promote the free interchange of ideas essential to scientific and industrial progress while ensuring that classified information is not compromised.

The Department of Energy Office of Declassification, working with various other groups, has been instrumental in the development of *10 CFR Part 1045 — Nuclear Classification and Declassification*, which provides a legislative (statute) basis for the classification and declassification system. This regulation for the first time publicly defines and implements government-wide requirements for the classification and declassification of Restricted Data and Formerly Restricted Data. It is available on the Internet: http://www.access.gpo.gov/nara/cfr/waisidx_99/10cfr1045_99.html.

Declassification Procedures

DOE M 475.1-1A provides details for classifying and *declassifying* information, documents, and material (along with other relevant information). See Chapter VI, Part B for procedures on declassification of a document or material.

Unclassified/Classified Computer Security

Because classified and unclassified computer and communications resources require different levels of protection, DOE federal and contractor organizations are responsible for developing and implementing the computer security programs, both classified and unclassified. Computer security plans must be written for all computers, both classified and unclassified. These plans must address all computer and communications resources, including mainframes, local area networks (LANs), communication networks, and mini- or microcomputers, regardless of whether or not classified matter is processed on each resource. Requirements for these security plans are specified in various DOE directives (e.g., DOE M 470.4-4, DOE M 471.2-2 *Classified Information Systems Security* 8-3-1999, DOE O 470.4 and DOE O 205.1 *Cyber Security Program,* 3-21-03).

The Classified Information System Security Plan (ISSP) and the Cyber Security Program Plan (CSPP) are the two security plans for, respectively, classified and unclassified information systems. The Classified ISSP and the CSPP are referenced in the contractor's Site Safeguards and Security Plan (SSSP). These security plans are to be coordinated, as appropriate, with other site programs (e.g., Classified Matter Protection and Control, Personnel Security, Physical Security, Communications Security).

The CSPP details the contractor's approach to ensuring protection of all *unclassified* DOE information and specified information systems. "Cyber security" refers to the protection of information systems against unauthorized access to or modification of information, against loss of accountability for information and user actions, and against the denial of service to authorized users. It includes those measures necessary to protect against, detect, and counter such threats. For more information, see DOE O 205.1.

Each DOE contractor is required to set up a computer management group. This computer management group has many responsibilities, including managing the assignment of user accounts (user IDs) that grant access to various resources, e.g., mainframes, networks, client/server systems, the Internet. This group is also responsible for the information-systems security education, awareness, and training activities for site personnel. The site supervisor, in concert with the computer management group, should provide information for site personnel about how to mark, handle, protect, and dispose of classified and sensitive-unclassified output and removable media in the appropriate manner. Subcontractor computer management groups will need to coordinate these responsibilities with the DOE LRO and /or the prime contractor's computer management group.

User Responsibilities (Classified Information Systems)

The FSO should be aware that contractor personnel who use classified information systems in performance of their duties (i.e., users) assume additional responsibilities. For example, users are usually required to

- Sign an acknowledgment of responsibility (Code of Conduct) for the security of classified information systems classified information.
- Attend training about the information system's prescribed security restrictions and safeguards prior to initial access to the system.
- Be aware of their responsibilities, accountable for their actions, and in compliance with computer and communications security protection requirements.
- Protect passwords and other access authentication mechanism (e.g. Personal Identification Numbers (PINs) and SECURID cards) with the same protection as that afforded the highest classification level/category

of the information it's protecting, and change them when compromised or potentially compromised.

- Protect their desktop computers from malicious code, e.g., viruses, worms and Trojan horses.

- Mark, handle, protect, and then dispose of classified and sensitive-unclassified output and removable media in the appropriate manner.

- Determine the sensitivity level of any data prior to generating information for use on a computer.

- Sanitize their information; processing equipment before changing processing environments (e.g., different classification levels or categories), according to site procedures. This includes desktop computers, terminals, workstations, word processors, file servers, and printers. Sanitization is the removal of information from media or equipment in a way that prevents data recovery by use of *any known technique* or analysis.
  NOTE: Sanitization must include the removal of data from the media or equipment, as well as the removal of all sensitivity or classified labels, markings, and activity logs.

- When an incident is suspected to have occurred, the facility where the incident occurred has 24 hours to examine and document all pertinent facts and circumstances to determine whether an incident has occurred. During this period, the incident must be categorized by an Impact Measurement Index (IMI) Number. If it is determined that an incident of security concern did not occur, no further action is required.

  1) Within 1 hour following categorization for the most serious security incidents determined to be IMI-1, the originating site/facility will transmit a DOE Form 471.1 *Security Incident Notification Report*, to the DOE EOC. Verbal notification may be made, and then followed-up with the transmission of DOE F 471.1.

  2) Within 8 hours following categorization of security incidents determined to be IMI-2/3, the originating site/facility will transmit a DOE F 471.1 to the DOE EOC.

  3) Within 30 days following categorization of security incidents determined to be IMI-4, the originating site/facility will report in a monthly "Roll up".

- Inform the organization's computer management group about any changes to their processing environments, e.g., a change in the classification level of data processed, movement of their information processing equipment into or out of a vault, a change in responsible user for a system, or sensitive and mission-essential processing.

- Report any use that may be waste, fraud, and/or abuse of government computing resources.

All computer and communications resources used by the DOE or on its behalf are for official government business. Audits and/or surveys of site automated information systems are conducted periodically to detect and deter waste, fraud, and/or abuse of government computing resources. Any use that is determined not to be official will be brought to the attention of the Office of Inspector General. In the case of a classified information system misuse, a security infraction or violation may be issued. Security infractions and the inquiry process are discussed in the next chapter.

Operations Security (OPSEC)

Information does not have to be classified to be valuable to an adversary. Seemingly insignificant bits and pieces of unclassified data can be gathered and analyzed to reveal sensitive or classified information. To an intelligence gatherer, nothing is irrelevant. Each piece of information is considered. If the obtained data does not fit the current scenario, it is kept for future reference.

The objectives of the Operations Security (OPSEC) program are to:

1) Ensure that critical/sensitive information is protected from compromise and secured against inadvertent, rather than intentional, disclosure. The program is structured to provide management with the information required to make sound risk management decisions concerning the protection of critical/ sensitive information.

2) The OPSEC process is designed to disrupt or defeat the ability of foreign intelligence or other adversaries to exploit sensitive Departmental activities or information. The process is also designed to prevent the inadvertent disclosure of such information.

3) It is essential to understand that OPSEC is concerned with protecting *both* classified *and* unclassified activities and information; hence the use of the phrase, "critical/sensitive Departmental activities or information." In some instances it is impossible to defeat an adversary's ability to exploit a vulnerability; nevertheless, it is often possible to disrupt and delay that effort, resulting in increased resource costs to the adversary and reduced effectiveness of his actions. Remember that OPSEC is concerned not only with the threat from foreign intelligence activities, but also with threats generated by any adversaries.

Our adversaries need information about DOE activities to gain a military, political, or economic advantage in pursuit of their goals. The Department's operations, the activities conducted daily -- communications, publications, records management, budget, procurement, travel, document and property disposal, and

physical operations -- are examples of sources of that information. OPSEC halts or reduces the flow of information about DOE activities by reducing the unnecessary dissemination of information associated with critical/sensitive programs or activities.

The OPSEC process produces its product – cost-effective OPSEC support to a total security program – from five basic steps:

1. Identification of the Critical Program Information (CPI) (Information someone wants, information we feel is crucial for our success)

2. Analysis of the threat [The adversary's ability to collect, process, analyze and use (my) information]

3. Assessment of vulnerabilities (Operational weaknesses, exploitable conditions, such as observable or detectable bits of information or changes in behavior that point to critical/sensitive information)

4. Assessment of risk (Evaluate your activities in terms of the identified operational weaknesses or exploitable conditions. How good are the adversaries? How big a risk will they take? How much damage could loss of critical information do? Such loss can lead to injury or death, damage, destruction, mission failure, loss of a technological or competitive edge, etc.)

5. Application of countermeasures (Anything that negates or reduces the ability of an adversary to exploit vulnerabilities)

Understanding the capabilities and limitations of the adversary is essential to any protection program. Similarly, identification of the information deemed most essential to keep from an adversary, the Critical Program Information, is necessary to determine what should be protected from the threat.

OPSEC awareness on the part of all members of the work force is a vital component of the OPSEC process. Personnel should be cognizant of the OPSEC program and, within the bounds of sound security practice, be aware of the threat to their organization and the information considered most significant. It is the role of the FSO to take the lead for instilling and enhancing OPSEC awareness among employees.

Review Questions for Chapter 4

1. In the United States, the two primary means of setting forth classification system regulations are _____ and _____.

   a. The Manhattan Project; the Cyber Security Protection Plan (CSPP)

   b. Statutes (legislation) passed by congress; Executive Orders (EOs)

   c. The Life Cycle Approach to Classification; Export Controlled Information (ECI)

   d. None of the above

2. How is the determination made as to whether information or material is – or is not – classified?

   a. NSI (National Security Information) is "born classified."

   b. An authorized classifier who is specially trained for the particular area can determine whether information or material is – or is not – classified.

   c. If it's "sensitive" (for example, UCNI, ECI, or OUO), it is classified.

   d. All the above

3. A classification level is assigned to classified information according to the potential for damage to national security if the information is disclosed to unauthorized persons. The three levels of classification are

   a. Classified, sensitive unclassified, and unclassified.

   b. Restricted Data (RD), Formerly Restricted Data (FRD), and National Security Information (NSI).

   c. Top Secret (TS), Secret (S), and Confidential (C).

   d. Secret, Confidential, and Company Proprietary.

4. The categories of classified information are dependent on the subject of the information. The three categories of classified information are

   a. Classified, Sensitive Unclassified, and Unclassified.

   b. Restricted Data (RD), Formerly Restricted Data (FRD), and National Security Information (NSI).

   c. Top Secret (TS), Secret (S), and Confidential (C).

   d. Secret, Confidential, and Company Proprietary.

5. Which of the following best describes the minimum markings for inside pages of classified documents?

   a. Classification level only (for all classified matter)
   b. Classification level for all classified matter and classification category (if NSI)
   c. Classification level for all classified matter and classification category (if RD or FRD)
   d. None of the above

6. "Certain unclassified but sensitive administrative information" describes which of the following?

   a. UCNI

   b. ECI

   c. OUO

   d. TS

7. "Sensitive government information that is controlled even though it is not classified because, if released, it could help a terrorist or saboteur gain access to nuclear materials or facilities" describes which of the following?

   a. UCNI

   b. ECI

   c. OUO

   d. TS

8. "Technical information that cannot be exported unless licensed by the Department of State, Department of Commerce, or the Nuclear Regulatory Commission" describes which of the following?

    a. UCNI

    b. ECI

    c. OUO

    d. TS

9. According to information presented in this chapter, which of the following is/are true of the declassification process?

    a. Reducing the amount of information in the classification system increases respect for the information that needs to stay protected.

    b. RD/FRD is *always* automatically declassified if it has a *Specific Date for Declassification* marking.

    c. NSI with a *Specific Date for Declassification* marking is *never* automatically declassified after the specified date or event has passed.

    d. All the above

    e. None of the above

10. According to the DOE directives discussed in this chapter, which of the following is/are true about the DOE contractor's written security/protection plan(s) for computer/communications systems?

    a. Only one security/protection plan document is required, because only classified computer/communications systems need protection.

    b. Two security/protection plan documents are required, because both classified and unclassified computer/communications systems require their own security/protection plan documents.

    c. The contractor's Site Safeguards and Security Plan (SSSP) must contain the security/protection plan document(s) for the site's computer/communications systems.

    d. a,c

    e. b,c

11. Which of the following are additional responsibilities assumed by personnel who use classified information systems in performance of their duties?

    a. Marking, handling, protecting, and then disposing of classified output and media in the appropriate manner.

    b. Sanitizing their information processing equipment before changing processing environment.

    c. Signing a Code of Conduct acknowledging responsibility for the security of classified information system classified information.

    d. All the above.

12. The objective(s) of the Operations Security (OPSEC) program is/are to

    a. help ensure that sensitive Departmental activities or information is protected from compromise and inadvertent disclosure.

    b. disrupt or delay the ability of foreign intelligence or other adversaries to exploit sensitive Departmental activities or information.

    c. protect both classified and unclassified sensitive activities and information.

    d. all the above.

13. Certain types of activities pose Operations Security (OPSEC) vulnerabilities because they lend themselves to inadvertent disclosure of sensitive information or activities. These include, but are not limited to

    a. telephone and e-mail communications.

    b. facsimile (fax communications).

    c. tossing into the trash documents containing sensitive information.

    d. professional publications or presentations.

    e. all the above.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 5: Incident Reporting, Inquiry Process, and Infractions

Goal

Upon completion of this chapter, students will have an awareness of the inquiry process associated with incidents of safeguards and security concern.

Objectives

Upon completion of this chapter, students will identify

1. The description of terms associated with the inquiry process.
2. Examples of infractions.
3. The time constraints imposed by DOE directives on responding to incidents of safeguards and security concern.
4. The agency to whom an incident is reported if an inquiry establishes that a violation occurred.
5. The agency to whom an incident is reported if an inquiry establishes credible information that fraud, waste, and/or abuse has occurred.
6. Examples of employee responsibilities in the inquiry process.
7. Characteristics of typical administrative contractor disciplinary actions of infractions.

The FSO may participate in some preliminary aspects of responding to incidents of safeguards and security concern, and may also be called upon to assist with the conduct of inquiries, as set forth in various DOE directives (e.g., See DOE O 470.4, *Safeguards and Security Program*, 8-26-05, DOE M 470.401, Chg.1, *Safeguards and Security Program Planning and Management*, 3-7-06, and DOE M 470.4-4, *Information Security*, 8-26-05.

Infractions

Infractions are, in general terms, knowing, willful, or negligent acts or omissions that do not constitute a violation of law or result in the actual compromise or the unauthorized disclosure that *could* reasonably be expected to result in an unauthorized disclosure of classified information.

Types of Incidents that may result in infractions

- Failure to properly store and protect classified documents or matter
- Loss of pass or badge because of negligence
- Failure to safeguard a computer access password
- Leaving an up-and-running computer workstation unattended at the close of business (or when the room is unattended), when it contains classified information or has access to a classified host computer
- Any attempt to obstruct justice

The Administrative Inquiry

An *inquiry* is an administrative proceeding to gather accurate, impartial facts about the incident of safeguards and security concern. An *inquiry* does *not* suspect intentional violation of criminal law. In contrast, an *investigation* is initiated to collect facts and evidence about a suspected violation of law, and is used to support criminal prosecution. Inquiries are *terminated* immediately upon discovery of credible evidence that an *intentional* violation of criminal law may have occurred. Inquiries must be kept separate from investigations.

- ❑ DOE S&S representatives who conduct administrative inquiries may *not* conduct investigations into *criminal* violations unless they are deputized agents of state or local law enforcement agencies, are in consultation with

the FBI, and are investigating criminal violations involving DOE and contractor activities, operations, or personnel.

Incidents of Safeguards and Security Concern

An *incident of safeguards and security concern* is an event that, at the time of occurrence, is of enough concern to warrant immediate review, inquiry, assessment, and reporting. The method and sequence for reporting and responding to an incident of safeguards and security concern will depend upon the situation as well as the immediacy of action that may be required to mitigate the situation. The following requirements may apply.

Response to Incidents of Safeguards and Security Concern

- **Discovery.** *Immediately* upon discovery, report to the *facility security officer* (FSO). Exercise care and caution regarding how the information is reported, because the facts or details may contain classified information.

  - The FSO has 24 hours to examine and document all pertinent facts and circumstances to determine whether an incident has occurred. During this period, the incident must be categorized by an Impact Measurement Index (IMI) Number. If it is determined that an incident of security concern did not occur, no further action is required. If an incident has occurred:

    (1) Within 1 hour following categorization for the most serious security incidents determined to be IMI-1, the originating site/facility will transmit a DOE Form 471.1 *Security Incident Notification Report*, to the DOE EOC. Verbal notification may be made, then followed-up with the transmission of DOE F 471.1.

    (2) Within 8 hours following categorization of security incidents determined to be IMI-2/3, the originating site/facility will transmit a DOE F 471.1 to the DOE EOC.

    (3) IMI-4's are reported on a monthly "Roll up" report.

- **Inquiry.** Final Inquiry reports must be within 60 working days of the initial discovery and Special Updates are submitted as required.

Documentation

- **Infractions.** Documentation of disciplinary action(s) taken for the incident. This action is commonly referred to as an "infraction."

- DOE F 5639.3, *Report of Security Incident/Infraction* is used to document security infractions. When infractions are issued, a copy of the DOE F 5639.3 is filed in the personnel security file.

- DOE F 5639.2 (formerly DOE F 5635. 11), *Reporting Unaccounted for Documents* is used to document incidents in which classified information is lost or unaccounted for. Please exercise care when using this form, because it may contain classified information.

❑ **Violations**

- When occurrence of a ***criminal violation*** is supported by credible evidence, and the inquiry process is terminated, the violation is reported through DOE channels to the Security Policy Staff and the local **FBI** office.

- When the loss, compromise, or unauthorized disclosure of a ***national security interest*** is supported by credible evidence and the inquiry process is *terminated* the incident is referred to the **FBI** and/or the appropriate law enforcement agency.

- When occurrence of **fraud, waste, and/or abuse** is supported by credible evidence and the inquiry process is terminated the incident is reported to the **Office of the Inspector General**.

Employee Responsibilities in the Inquiry Process

The FSO is responsible for raising employees' awareness of their responsibilities in the inquiry process. These responsibilities may include the following:

❑ *Immediately* upon discovery, reporting to the *facility security officer* (FSO) information that classified matter has been or may have been lost or compromised or is otherwise unaccounted for.

❑ Immediately reporting all other actual or suspected security infractions to the DOE or the prime contractor's security point of contact.

❑ Complying with safeguards and security requirements established in the DOE directives and the site-specific safeguards and security procedures.

❑ Cooperating fully with an employer's inquiry into a job-related misconduct, because an employer is legally entitled to interview an employee concerning a violation of policy or procedure.

Disciplinary Actions for Infractions

When a non-criminal infraction occurs, disciplinary actions—rather than criminal penalties—may be imposed on the employee. Infractions involve failure to comply with prescribed security procedures or directives for the proper protection of classified information or matter.

- For contractor employees, disciplinary or corrective action will be determined by appropriate management officials according to the contractor's personnel policies and procedures.

- This management decision may vary in its formality from disciplinary action by the employee's supervisor for less severe infractions to formal disciplinary proceedings for more severe ones. In all instances, consideration is given to the nature and severity of the infraction.

FSOs and the Inquiry Process

Significant legal issues are associated with inquiries into incidents of safeguards and security concern that are beyond the scope of this chapter. FSOs may wish to take additional training such as NTC's *Legal Aspects of Inquiries* (ISC-202DV) correspondence course to further enhance understanding of the inquiry process (see http://www.ntc.doe.gov for course information).

Review Questions for Chapter 5

1. A/an _____ is a criminal proceeding initiated to collect facts and evidence about suspected violations of criminal law.

    a. infraction
    b. investigation
    c. inquiry
    d. None of the above

2. A/an _____ is a knowing, willful, or negligent act or omission involving failure to comply with prescribed security procedures or directives for the proper protection of classified information or matter.

    a. violation
    b. investigation
    c. inquiry
    d. None of the above

3. An _____ is an administrative proceeding conducted to collect facts and evidence about incidents of safeguards and security concern, such as lost or missing documents, in which a violation of criminal law is not suspected.

    a. infraction
    b. investigation
    c. inquiry
    d. None of the above

4. Which of the following are examples of security incidents that could result in an infraction (as presented in this chapter)?

    a. At the close of business, leaving an up-and-running computer workstation unattended when it contains classified information or has access to a classified host computer
    b. Removal of classified documents or matter from a security area without proper authorization
    c. Improper transmission of classified documents or matter
    d. All the above

5. Following notification that classified matter has been or may have been lost or compromised or is otherwise unaccounted for, *when is* the FSO required to initiate a report?

    a. Immediately
    b. By close of business (COB)
    c. Within 24 hours
    d. 8 hours

6. When an inquiry establishes that a criminal *violation* has occurred, the incident is

    a. reported to the Federal Bureau of Investigation and/or the appropriate law enforcement agency (for investigation) by the cognizant DOE Security Policy Staff.
    b. reported to the Office of the Inspector General (for investigation).
    c. reported to the employee's supervisor (for investigation).
    d. None of the above

7. When an inquiry establishes credible information that fraud, waste, and/or abuse has occurred, the incident is

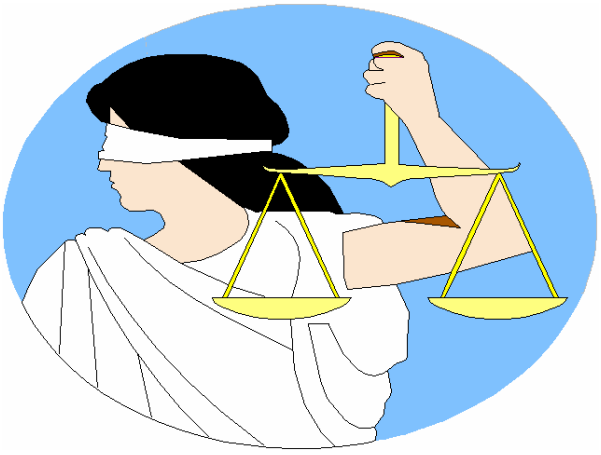
    a. reported to the Federal Bureau of Investigation and/or the appropriate law enforcement agency (for investigation).
    b. reported to the Office of the Inspector General (for investigation).
    c. referred to the employee's supervisor (for investigation).
    d. None of the above

8. Which of the following is/are examples of employee responsibilities in the inquiry process?

    a. Cooperate fully with an employer's inquiry into job-related misconduct.
    b. Comply with safeguards and security requirements established in the DOE directives.
    c. Comply with safeguards and security requirements established in the site-specific safeguards and security policy and procedures.
    d. Immediately report all actual or suspected security infractions.
    e. All the above

9. Which of the following are characteristics of typical administrative (contractor) disciplinary actions for infractions?

   a. Disciplinary action is determined by appropriate management officials according to the contractor's personnel policies and procedures.
   b. Criminal penalties are imposed on the employee.
   c. This management decision may vary in its formality.
   d. Consideration is given to the nature and severity of the infraction.
   e. a, c, d



Chapter 6: Other Related Programs

Goal

Upon completion of the chapter, students will have an awareness of physical protection requirements, Materials Control and Accountability (MC&A), and requirements for reporting fraud, waste, and abuse.

Objectives

Upon completion of this chapter, students will identify the following:

The types of DOE security areas.

1. Examples of prohibited articles.
2. Examples of controlled articles.
3. The two basic elements of the MC&A program.
4. Three materials designated as special nuclear material (SNM) by DOE
5. The meaning of the term “graded safeguards” for nuclear materials.
6. Two of the factors that determine the level of protection provided for SNM.
7. The primary MC&A duties of the nuclear materials custodian.
8. Examples of criminal waste, fraud, and abuse for which reporting to the OIG is required.
9. Examples of fraud, waste, fraud, and abuse for which reporting through the supervisory chain is appropriate.
10. Examples of violence in the workplace.

Physical Security

Physical security is one component of the DOE's Safeguards and Security Program that was established to ensure that appropriate levels of protection consistent with the risks and consequences are provided to DOE assets against various acts.

Security Areas

The term *security area* refers to any area containing Department of Energy safeguards and security interests that require physical protection measures. DOE facilities typically have a series of physical spaces designated as security areas surrounding a designated S & S interest. These security areas; i.e., property protection, limited, exclusion, protected, vital, and material access areas, provide for the imposition of varying or graded physical protection measures which entail controlling access to and egress from the designated areas and security. The security areas include:

– Property protection area (PPA)

– Limited area (LA)

– Exclusion area (EA)

– Protected area (PA)

– Vital area (VA)

– Material access area (MAA)

The type of security area required for a given DOE asset is dictated by the level of protection it requires. DOE M 470.4-2 and DOE M 470.4-7 should be referenced for additional information.

- PPAs — *Property protection areas* are established areas having defined boundaries and access controls for the protection of DOE property. Protection measures shall be adequate to give reasonable assurance of protection for the assets and Departmental property.

- LAs — *Limited areas* are security areas having boundaries defined by physical barriers, used for the protection of classified matter and/or Category III quantities of special nuclear material, where protective personnel or other internal controls can prevent access by unauthorized people to classified matter or special nuclear material. Security officers, security police officers, or other internal security measures provide the necessary means to control access.

- EAs — *Exclusion areas* are security areas defined by physical barriers and subject to access control where mere presence in the area would normally result in access to classified information.

- PAs — *Protected areas* are security areas defined by physical barriers (i.e., barriers, walls or fences) and surrounded by intrusion detection and assessment systems, to which access is controlled, used to protect Category II special nuclear material and classified matter and/or to provide a concentric security zone surrounding a material access area or a vital area.

- VAs — *Vital areas* are security areas located within a protected area possessing a separate perimeter and access controls to afford layered protection, including intrusion detection, for vital equipment, systems, or components whose failure or destruction would cause unacceptable interruption to a national security program or harm to the health and safety of the public.

- MAAs — *Material access areas* are security areas that are approved for the use, processing, and/or storage of a Category I quantity or other quantities of special nuclear material that can credibly roll-up to a Category I quantity and which has specifically defined physical barriers, located within a protected area, and is subject to specific access controls.

Prohibited and Controlled Articles

When entering most DOE facilities, all personnel must comply with the prohibited (i.e., any item administratively restricted from being introduced into a security area) and controlled articles requirements.
The following articles are prohibited from all DOE security areas:

- Dangerous weapons

- Explosives

- Instruments or material likely to produce substantial injury or damage to persons or property

- Controlled substances, e.g., illegal drugs and associated paraphernalia, but not prescription medicine

- Other items prohibited by law. Specific information covering prohibited items may be found under the provisions of 10 Code of Federal Regulations (CFR) 860 and 41 CFR 101-20.3.

The following privately owned articles are *controlled* and are not permitted in a limited area, exclusion area, protected area, vital areas, or material access area without prior authorization.

- Recording equipment (audio, video, optical, or data)
- Portable electronic devices equipment capable of recording information or transmitting data information system (any piece of equipment with a data exchange port capable of being connected to automated information system equipment)
- Cellular telephones and radio frequency transmitting equipment
- Computers and associated media
- Alcohol

All articles shall be controlled because of their potential to be used to record or transmit information without authorization.

NOTE: Authorization for use of such devices in one security area does not apply to all other security areas.

FSOs may be interested in NTC's *Introduction to Physical Security Systems* (PHY-100DB) Correspondence Course for further enhancement of basic knowledge. NTC also offers several other courses on physical protection topics (see http://www.ntc.doe.gov).

Materials Control and Accountability (MC&A)

Materials Control and Accountability (MC&A) is another important element of the Safeguards and Security (S&S) Program. MC&A is the practice of controlling and accounting for nuclear materials that are important to national security.

Before a facility is allowed to handle nuclear materials, it must first meet certain DOE standards and be approved as a nuclear facility. Each site is required to develop its MC&A Program procedures according to DOE requirements, e.g., DOE O 470.4., DOE M 470.4-6.

Nuclear Materials

The types of nuclear materials that some facilities maintain and safeguard include the following:

- Special nuclear material (SNM) is of particular concern to DOE because SNM can be made into nuclear weapons. DOE has specifically identified three materials as SNM, because they can be

used to make a nuclear device. These include plutonium, uranium-233, and uranium that has been enriched in the isotope 235.

- Source nuclear materials used to produce SNM, e.g., thorium and naturally occurring uranium.

- Other nuclear materials used in either the nuclear weapons themselves or in the nuclear weapons program. (Tritium is a radioactive example; lithium is a nonradioactive example.)

Graded Protection

DOE has developed a "graded" concept for providing safeguards and security, because some DOE assets would have a far more serious impact on the national security, the health and safety of DOE and contractor employees, the public, and/or the environment than others, if loss, theft, compromise, and/or unauthorized use occurred. In keeping with the graded safeguards concept, facilities may operate under varying safeguards requirements due to different material types, forms, quantities and flows. To comply with the DOE graded safeguards concept the facility shall have controls to assure the following:

1. A system designed to provide varying degrees of physical protection, accountability, and material control to different types, quantities, physical forms, and chemical or isotopic compositions of nuclear materials consistent with the risks and consequences associated with threat scenarios.

2. A system designed to provide the greatest relative amount of control and effort to the types and quantities of special nuclear material that can be most effectively used in a nuclear explosive device.

Therefore, the policies and S&S measures (level of effort and resources) that are applied in a proportional manner toward the protection of S&S interests based on; the quantities and types of nuclear materials being produced, stored, used, or processed; the impact of their loss, destruction, or misuse.

DOE uses a classification system to indicate the security requirements for protection of varying types and amounts of SNM, because some forms of nuclear materials are more desirable to adversaries. This classification system divides SNM into categories (i.e., Category I, Category II, Category III, and Category IV) and attractiveness levels (A to E). In general, the category is based on the quantity of material present, and the attractiveness level is determined by the effort required to convert that material into an improvised nuclear device. For SNM, the greatest protection is given to Category I materials, with lesser protection required for Categories II and III, and only minimal protection for Category IV materials. Similarly, greater protection is afforded to Attractiveness Level A materials than to Attractiveness Level E materials.

One of the primary purposes of the MC&A program is to minimize the threat of proliferation of nuclear weapons by tracking and controlling materials used in their manufacture. Therefore, protecting special nuclear material is a high priority in DOE.

Nuclear Materials Custodian

The quantity of nuclear materials must be known and continuously monitored in order to control and account for nuclear materials, and to verify that none has been diverted or stolen. Nuclear materials are assigned to various areas within a facility. These areas are called Material Balance Areas (MBAs). One person within each MBA is responsible for the control and accountability of all nuclear material in that area. This individual is called the nuclear materials custodian.

Periodic physical inventories are conducted on all nuclear material to provide assurance that all nuclear material is present and accounted for.

When personnel have questions about nuclear materials in the work area, the FSO should ask them to contact the nuclear materials custodian for that area.

Personnel who work with nuclear materials must follow strict DOE policies and procedures. Only properly trained workers may handle, transport, store, assay, or process nuclear materials. Typically, workers are required to follow standard operating procedures (SOPs) for all nuclear materials work. Entry control both into and out of nuclear materials security areas may require workers to pass through radiation detectors.

Reference DOE O 470.4 and DOE M 470.4-6 for more information on MC&A and DOE O 470.4 for more information on graded protection. FSOs may be interested in NTC's MCA-101DC *Introduction to Nuclear Materials Control and Accountability* CBT (computer-based training) for further enhancement of their understanding of MC&A. NTC also offers numerous other MC&A-related courses for the DOE community (see http://www.ntc.doe.gov).

Fraud, Waste, and Abuse

Important note: The fraud, waste, and abuse reporting requirement does NOT apply to information about espionage, which should be reported to the Office of Counterintelligence.

DOE N 221.10 notifies all DOE employees of their duty to report allegations of fraud, waste, and abuse to the Office of Inspector General, Office of Investigations, particularly if these violations are criminal in nature or show gross mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health or safety. Examples of criminal violations include, but are not limited to, false statements, false claims, bribery, kickbacks, fraud, theft, computer crimes, and conspiracy to commit any of these acts. The

policies and procedures for reporting fraud, waste, abuse, or corruption to the Department of Energy, Office of Inspector General are established in DOE O 221.1. The Department of Energy policy for cooperating with the Office of the Inspector General has been established in DOE O 221.2.

Noncriminal fraud, waste, and abuse violations normally should be reported through the supervisory chain, but may be reported to the Ethics Counselor in the Office of General Counsel or directly to the Office of Inspector General, Office of Investigations.

The following examples could apply:

Misusing government property

Charging personal long-distance telephone calls to the company or government telephone account (this includes direct dialing personal long-distance calls from a government owned telephone with long-distance access)

Using company/government owned fax machines to advertise or solicit for a private business

Using company/government mail services for personal mail

Taking home company/government owned supplies or equipment

Using company/government computers for accessing non work-related sites on the Internet or for other than official business without authorization

Making illegal copies of computer software

Using a government vehicle for non work-related trips

Gambling on company operated property, e.g.,

operating a football pool on the office computer

conducting or taking part in an office lottery

playing a card game for money

selling or buying a numbers slip or ticket

gambling on the Internet

Personnel with knowledge of fraud, waste, or abuse must inform the appropriate authority upon obtaining such information.

DOE O 442.1A and DOE G 442.1-1 establishes an independent avenue for reporting DOE and DOE- contractor employee concerns within the DOE Employee Concerns Program (ECP). The intent is to help foster a free and open

expression of employee concerns that results in an independent, objective evaluation of those concerns. FSOs should be aware of the DOE Whistleblower Protection Rule (10 CFR 708, accessible at http://www.oha.doe.gov/regs/rule708/031000Rule.html),

(10 CFR 708, accessible at http://www.washingtonwatchdog.org/documents/cfr/title10/part708.html), which requires, among other things, that employers (including contractors) inform their employees about the "Whistleblower Protection Program," and post in conspicuous places at the worksite the name and address of the DOE office where a complaint can be filed. For example, this might be a local DOE Employee Concerns Hotline or the OIG Hotline (Office of Inspector General).

Office of Inspector General

To contact the Office of Inspector General Hotline, DOE and DOE-contractor employees may use one of three OIG numbers to contact the office. These numbers are:

1-800-541-1625 (toll free)

202-586-4073 (commercial)

To file a complaint in writing, employees may contact the local DOE Office of Employee Concerns Manager or

E-mail: ighotline@hq.doe.gov

Fax: 202-586-4902

U.S. Office of Special Counsel

Disclosures of information evidencing violations of law, rule or regulation, gross mismanagement, gross waste of funds, abuse of authority, or a danger to public health or safety may be reported in confidence to (and the appropriate form requested from)

Disclosure Unit
U.S. Office of Special Counsel
1730 M Street, N.W., Suite 218
Washington, D.C. 20036-4505
Tel: (800) 572-2249
(202) 254-3640

Internet sites that may be of value to FSOs:

www.osc.gov/forms.htm
This is the U.S. Office of Special Counsel (OSC) Website page for Forms and Publications. Available forms include the Complaint Form and the Whistleblower Disclosure Form. Also available are various employee information programs with PowerPoint slide presentations and presenter's guides. Numerous publications provide useful information on many aspects of the Whistleblower Protection Program.

http://www.osc.gov/wbdisc.htm
This is the U.S. Office of Special Counsel (OSC) Whistleblower Disclosure Hotline

www.whistleblower.org/
The last button on this page is "Survival Tips for Whistleblowers," which may be of interest in providing insight on the whistleblower process once it has been initiated. NOTE: Inclusion of this site is for informational purposes only and should in no way be construed as an endorsement of the site's sponsoring organization.

Violence in the Workplace

Workplace violence within DOE facilities is prohibited; violent behavior and threats are unacceptable conduct. Additional information about Workplace Violence Risk Factors and Prevention Strategies can be located at http://www.cdc.gov/niosh/violcont.html

Violence in the workplace is a serious safety and health issue. Its most extreme form, homicide, is the fourth-leading cause of fatal occupational injury in the United States. According to the Bureau of Labor Statistics Census of Fatal Occupational Injuries (CFOI), there were 551 workplace homicides in 2004 in the United States, out of a total of 5,703 fatal work injuries. Environmental conditions associated with workplace assaults have been identified and control strategies implemented in a number of work settings. For example, OSHA has developed guidelines and recommendations to reduce worker exposures to this hazard but is not initiating rulemaking at this time.

Congress passed the Occupational and Safety Health Act of 1970 (the OSH Act, or the Act), to ensure worker and workplace safety. Their Goal was to make sure employers provide their workers a place of employment free from recognized hazards to safety and health, such as exposure to toxic chemicals, excessive noise levels, mechanical dangers, heat or cold stress, or unsanitary conditions. OSHA does not have a specific standard for workplace violence. However, under the Occupational Safety and Health Act, the extent of an employer's obligation to address workplace violence is governed by the General Duty Clause, as follows:

Section 5(a)(1) of the OSH Act, or P.L. 91-596 (the "General Duty Clause") provides that

"Each employer shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees." 29 U.S.C. 654(a)(1)

Note: Twenty-four states, Puerto Rico and the Virgin Islands have OSHA-approved State Plans (see http://www.osha.gov/fso/osp/index.html) and have adopted their own standards and enforcement policies. For the most part, these States adopt standards that are identical to Federal OSHA. However, some States have adopted different standards applicable to this topic or may have different enforcement policies.

In its commitment to encourage employers to develop workplace violence prevention programs, in 1996 and 1998 OSHA published guidelines for preventing workplace violence for various industries. Although not exhaustive, OSHA's guidelines and recommendations include policies, procedures, and corrective methods to help prevent and mitigate the effects of workplace violence.

Duty to Warn

Some contractor organizations have standards of employee conduct which state that employees have a "duty to warn" their supervisors, security personnel, or HR Department representatives of any suspicious workplace activity or situations or incidents that they are aware of that involve potentially problematic employees, visitors, customers, or former employees. Examples of problematic behavior include but are not limited to the following:

Physical contact with another person that is hostile or aggressive

A statement that is threatening

A gesture that threatens harm to another person

Intimidation

Offensive remarks

Acts of violence

Other aggressive behavior

A course of conduct that would cause a reasonable person to believe that he or she is under threat of harm

Review Questions for Chapter 6

1. Two types of DOE Security Areas are

   a. Protected Area and Material Access Area.
   b. Material Accounting Area and Material Control Area.
   c. Restricted Access Area and Cleared Access Area.
   d. General Access Area and Classified Area.

2. Which of the following are examples of *prohibited* articles in all DOE security areas?

   a. A dangerous weapon
   b. A dangerous explosive
   c. Recording equipment (audio, video, optical, or data)
   d. All the above
   e. a, b

3. Which of the following are examples of *controlled* articles?

   a. A dangerous weapon
   b. Alcohol
   c. Controlled substances, e.g., illegal drugs
   d. All the above
   e. b, c

4. The two basic elements of the MC&A program are

   a. materials control, materials production.
   b. materials accounting, materials production.
   c. materials control, material destruction.
   d. materials control, materials accounting.

5. The three materials designated as special nuclear material (SNM) by the DOE are

   a. plutonium, nuclear compounds, enriched oxides.
   b. tritium, radioactive isotopes, uranium-130.
   c. plutonium, uranium-233, and uranium enriched in the isotope 235.
   d. source nuclear material, special nuclear material, other nuclear materials used in the process of making nuclear weapons.

6. “Graded safeguards” for nuclear materials refers to _____.

    a. the safeguards evaluation program
    b. a system for categorizing sites by their functions
    c. an assessment of a site's vulnerability to various threat scenarios
    d. providing varying levels of protection, accountability, and controls based on the quantity and type of nuclear materials being used, stored, or processed

7. The classification system used for indicating the security requirements for protection of SNM is based on two SNM factors, _____ and _____.

    a. the *function* of the facility, the measurable *radiation levels* of materials on site
    b. the *function* of the facility, the *type* of nuclear material on site
    c. the *category* of nuclear material on site, the attractiveness level of nuclear material on site
    d. the *weight* of nuclear material on site, the measurable *radiation levels* of materials on site

8. The primary MC&A duties of the nuclear materials custodian are

    a. materials control, materials dissolution.
    b. materials control, materials production.
    c. materials accounting, materials production.
    d. none of the above.

9. Which of the following are examples of criminal fraud, waste, and abuse for which reporting to the OIG is appropriate?

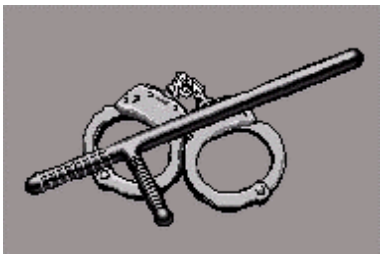
    a. Kickbacks
    b. Theft of government property
    c. Bribery of coworkers
    d. All the above
    e. a, b

10. Which of the following are examples of fraud, waste, and abuse for which reporting *through the supervisory chain* might be appropriate?

    a. Using company fax machines
    b. Taking part in an office lottery
    c. Bribery of coworkers
    d. All the above
    e. a, b

11. According to information presented in this chapter, which of the following are examples of violence in the workplace?

    a. A statement that is threatening
    b. A body gesture that threatens harm to another person
    c. Intimidation
    d. Physical contact with another person that is hostile or aggressive
    e. All the above



THIS PAGE INTENTIONALLY LEFT BLANK